ETSI GS ISI 002 V1.2.1 (2015-11)

Information Security Indicators (ISI);
Event Model
A security event classification model and taxonomy

Reference
RGS/ISI-002ed2

Keywords
ICT, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Information Security Indicators (ISI).

The present document is included in a series of 6 ISI specifications. These 6 specifications are the following (see figure 1 summarizing the various concepts involved in event detection and interactions between all parts):

- ETSI GS ISI 001-1 [i.3] addressing (together with its associated guide ETSI GS ISI 001-2 [i.4]) information security indicators, meant to measure application and effectiveness of preventative measures.
- The present document (ETSI GS ISI 002) addressing the underlying event classification model and the associated taxonomy.
- ETSI GS ISI 003 [i.11] addressing the key issue of assessing an organization's maturity level regarding overall event detection (technology/process/ people) in order to evaluate event detection results.
- ETSI GS ISI 004 [i.12] addressing demonstration through examples how to produce indicators and how to detect the related events with various means and methods (with a classification of the main categories of use cases/symptoms).
- ETSI GS ISI 005 [i.13] addressing ways to produce security events and to test the effectiveness of existing detection means within organizations (for major types of events), which is a more detailed and a more case by case approach than in ETSI GS ISI 003 [i.11] and which can therefore complement it.

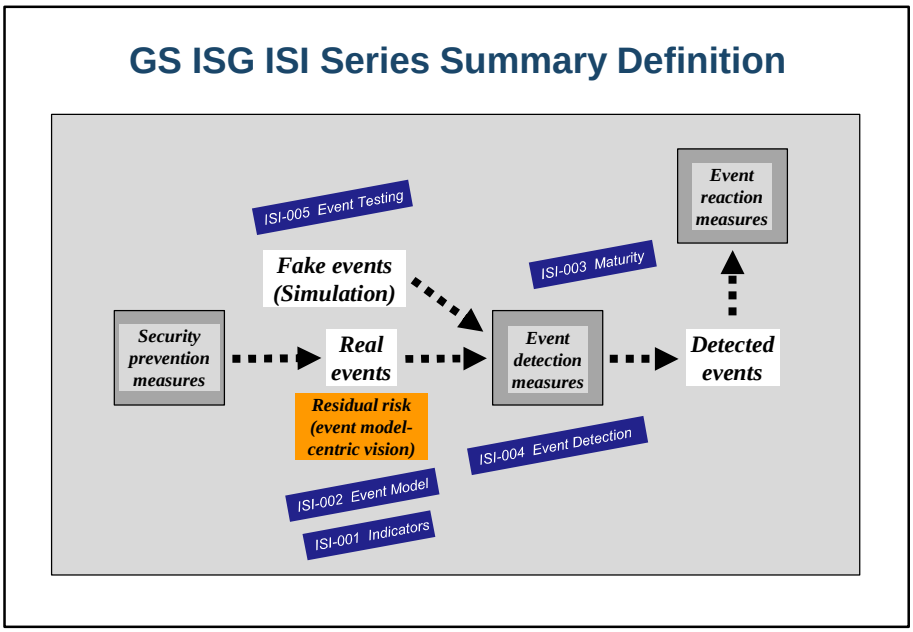

Figure 1: Positioning the 5 GS ISI against the 3 main security measures

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

A corporate Cyber Defence and SIEM approach implements continuously security improvements with the main goals to:

- operationally and constantly reduce the **residual risk** incurred by their Information Systems (see figure 2, which highlights the two associated types of events - incidents and vulnerabilities - and the joint area covered by IT security policy through the concept of usage or implementation drift); and
- to assess the actual **application** and real **effectiveness** of their **security policies** (or of their ISMS, if they have one), for the purpose of their constant improvement.

Such an approach, which to a large extent relies on using the traces available in the Information System's various components, is organized around an **"event-model centric"** vision, and can also be tied up to the PDCA model that is commonly used in quality and security areas. As such, this primarily involves implementing this model's PDCA "Check" step on the basis of very detailed knowledge of threats and vulnerabilities.

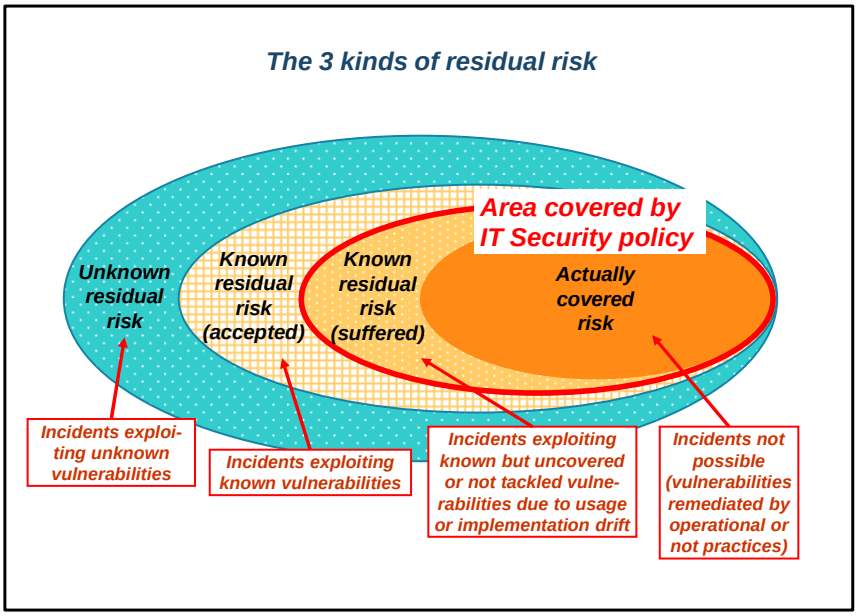

Figure 2: The 3 kinds of residual risks

Worldwide trends in ICT security show that significant progress can be accomplished within a few years with the deployment of an organization-wide operational Cyber Defence and SIEM approach. A recent survey by a major consulting firm of 15 major companies and organizations brings to light nine key success criteria. The two most important criteria are:

- The reliance of the Cyber Defence and SIEM approach on a security event classification model that takes into account both incidents and vulnerabilities, and that stresses particular attention to malicious and intentional acts, the monitored events themselves being selected on the basis of main relevant CIA risks and associated metrics (e.g. statistics).
- Training with this model for the relevant people using the Information System, with particular attention to the presentation of concrete examples of disasters associated with inventoried security event main types.

As such, the present document's objective is to build a **full taxonomy** to thoroughly describe all IT security events (and when appropriate and necessary non-IT security events) and, based on this, to present an **original representation** that leverages the current international best practices and enables diversified and complex uses. The choice of a detailed taxonomy, which describes security events through a set of attributes (different for incidents and vulnerabilities), ensures that all possible situations can be taken into account with the required flexibility (especially thanks to the provided open dictionary), while the representation chosen for the taxonomy, highlighting the main categories generally accepted by industry consensus, makes the event classification model easier to understand and embrace for stakeholders.

The present document is based on work carried out by the Club R2GS®, a French association created in 2008, specializing in Cyber Defence and Security Information and Event Management (SIEM), gathering large French companies and organizations (mainly users). The present document (ETSI GS ISI 002), as well as the other GS of ISG ISI, are therefore **based on a strong experience**, this community of users having adopted and used the event classification model and the related reference framework for indicators for more than three years on a national and world-wide scale.

1 Scope

The present document provides a comprehensive security event classification model and associated taxonomy (based on existing results and hands-on user experience), covering both security incidents and vulnerabilities. The two latter ones become nonconformities when they violate an organization's security policy. The present document mainly supports operational security staff in their effort to qualify and categorize detected security events, and more generally all stakeholders (especially CISOs and IT security managers) in their needs to establish a common language.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] NIST SP 800-126 Revision 2 (September 2011): "The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2".

[i.2] MITRE CCE List Version 5.20120314 (March 2012): "Common Configuration Enumeration".

[i.3] ETSI GS ISI 001-1: "Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture".

[i.4] ETSI GS ISI 001-2: "Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1".

[i.5] ISO/IEC 27000:2012: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.6] draft-ietf-mile-rfc5070-bis-11: "The Incident Object Description Exchange Format v2".

[i.7] ISO 27002:2013: "Information technology -- Security techniques -- Code of practice for information security management".

[i.8] ISO 27004:2009: "Information technology -- Security techniques -- Information security management -- Measurement".

[i.9] ISO 27005:2011: "Information technology -- Security techniques -- Information security risk management".

[i.10] FIRST Classification (November 2004): "CSIRT Case Classification (Example for enterprise CSIRT)".

[i.11] ETSI GS ISI 003: "Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection".

[i.12] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

[i.13] ETSI GS ISI 005: "Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply (ISO/IEC 27000 [i.5] compliant where applicable):

NOTE: See also the summary chart at the end of this list.

asset: information asset that has value to the organization and that can be broken down in primary assets (such as business activities, data, application software, etc. which hold the business value) and secondary/supporting assets (network or system infrastructure, which host primary assets)

assurance: refers to the planned and systematic activities implemented in a management system so that management requirements for a service will be fulfilled

NOTE: It is the systematic measurement, comparison with a standard, monitoring of processes and an associated feedback loop that confers error prevention. This can be contrasted with Management "Control", which is focused on process outputs.

base measure: regarding the "indicator" issue, a base measure is defined in terms of an attribute and the specified measurement method for quantifying it (e.g. number of trained personnel, number of sites, cumulative cost to date)

NOTE: As data is collected, a value is assigned to a base measure.

continuous auditing: periodic verification and collection of a series of controls identified within the Information System, corresponding with the detection of incidents and of software, configuration, behavioural or global security framework vulnerabilities and/or non-conformities

NOTE: There are three checking levels (in principle, hierarchy notably implemented within banking and financial institutions):

- Detailed behavioural, global security framework or technical checking at the security software or equipment level (network, system, application software).
- Level 1 checking via monitoring of trends and deviations of a series of significant measurement points.
- Level 2 checking (verification of existence of a satisfactory assurance and coverage level of the chosen control and measurement points, and of implementation of regulatory requirements).

Continuous auditing can be either manual or automatic (for example, monitoring by means of tools appropriate for a SIEM approach). Finally, continuous auditing is generally associated with statistical indicators (levels of application and effectiveness of security controls), that provide information regarding the coverage and assurance level of the security controls in question.

criticality level (of a security event): level defined according to the criteria which measures its potential impact (financial or legal) on the company assets and information, and which make it possible to evaluate the appropriate level of reaction to the event (incident treatment or vulnerability or nonconformity removal)

NOTE: The criticality level of a given event is determined by the combination of its severity level (inherent to the event itself - see definition below) and of the sensitiveness of the target attacked or concerned (linked to the asset estimated value for the company - whose value concerns confidentiality, integrity or availability). This concept of criticality level (usually defined on a scale of four levels) is at the core of any SIEM approach, for which classifying security events processing according to organization-defined priorities is vital from both a security and economic point of view.

derived measure: regarding the "indicator" issue, a measure that is derived as a function of two or more base measures

effectiveness (of security policy or of ISMS): as a supplement to the actual application of security policy (or of ISMS) and of its measures assessment, it is necessary to assess its level of effectiveness, that can be estimated through identified residual risk (that corresponds with the residual vulnerabilities that are actually exploited and that have led to security incidents)

NOTE: It should be added that the term "efficiency" is sometimes also used, but generally with a different meaning of economy in the use of resources (not addressed here for reasons of lesser relevancy).

(security) incident: single unwanted or unexpected security event, or series thereof, that correspond to the exploitation of an existing vulnerability (or attempt to), and with an actual or potential threat (attempt underway), that have a significant probability of compromising business operations and threatening information security

NOTE: In case of success, an incident affects nominal operations of all or part of an information system (according to the Confidentiality, Integrity and Availability criteria - English acronym CIA). An incident that manifests itself through previously unseen phenomena, or is built as a complex combination of elementary incidents often cannot be qualified and therefore inventoried or categorized easily; such an incident will often be referred to as an anomaly.

indicator: measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to a defined information need

NOTE: Indicators are the basis for analysis and decision making.

log: continuous recording of software usage computer data, with specific characteristics: detailed and specified structure, time-stamping, recording as soon as they occurs in files or other media

NOTE: Logs are a kind of trace (more general concept - see definition below).

non-conformity: security event that indicates that organization's required security rules and regulations have not been properly enforced, and are therefore the consequence of a usage or implementation drift

NOTE: Continuous monitoring of non-conformities (similar to continuous auditing - Cf. this term above) enables to better ensure that an organization's security policy is being enforced. Non-conformity can be further refined according to their kind: configuration, behaviour, global security (technical and organizational) and material. Non-conformities are also vulnerabilities or incidents, depending on the situation (see definition).

periodic audit (Periodic scanning): using isolated audit means, periodic acquisition and verification of security controls

NOTE: A periodic audit can also be either manual or automatic (for example, carried out through scanner type tools). Finally, a periodic audit is generally Boolean (all or nothing compliance level).

risk: product of the probability of occurrence of a security incident involving a specific asset by its impact on this asset (impact assessed according to the CIA sensitivity level)

NOTE: The level of risk exposure (concept which is used in risk assessment methods) corresponds to the product of the vulnerability level of the asset in question by the threat level hanging over it.

risk not covered (by existing security measures): Risk sometimes also referred to as "residual", which breaks down into 3 shares:

- Known and realized suffered risk, corresponding to the impact suffered by the organization under attack when the security policy is not applied (configuration, behavioural or global security non-conformities), and when known and critical software vulnerabilities are not appropriately addressed.
- Known and accepted risk that corresponds to a risk taken by choice by an organization, by comparing the risk associated with attacks with economic, usage and security level considerations.
- Unknown risk associated with unknown and unpatched vulnerabilities, or innovative attack vectors.

security event: information about a change of state in a system that may be security relevant and that indicates the appearance of a risk for the organization

NOTE: A security event is either an incident or a vulnerability occurrence or detection (see definition of these terms). 500 security events have been inventoried within the industry, and are grouped into 9 different major categories, with the 3 first corresponding to incidents, and the 4 last to vulnerabilities: external attacks and intrusions, malfunctions, internal deviant behaviours, behavioural vulnerabilities, software vulnerabilities, configuration vulnerabilities, general security (technical or organizational) vulnerabilities.

severity level (of security incident): Level (generally defined on a 4-element scale) inherent to the event itself and that depends on several criteria that vary according to the types of events (in decreasing order of importance):

- *Dangerousness* is the result of multiple factors with variable combinations according to circumstances or types of incidents: propagation speed for a worm, virulence, effectiveness, importance and number of impacted assets, capability of harm, target reachability, capability of remote action, persistence, weakness or lack of curative means, and extend of compromise (depth of component which is can be or has been reached, concept of Defence in Depth or DiD).
- *Stealthiness* covers the level to which the incident can be hidden to the defender: obvious visibility, visible through simple and easy to use mechanisms, detection requires advanced technical tools, almost invisibility. It is a key factor for monitoring and detection. Anonymization and camouflage, or active and passive masking techniques are stealthiness techniques. Stealthiness takes on an indirect meaning when it applies to similar not yet detected incidents.
- *Feasibility* relates to the attacker's motivation and skills. It increases proportionally to all the necessary prerequisites (regarding skills, tools, financial means, collusion, initial access, etc.) combined with the presence of exploitable vulnerabilities; feasibility can be tied often to the frequency of attacks that can be detected in the world. Its assessment is not simple, because it is subject to change. For example, it may be difficult to create a hacking tool for a given vulnerability. However, once the tool is released on the Internet, it can be used by unskilled attackers. Feasibility takes on an indirect meaning when it applies to a potential threat (see definition of this term), as the analysis of its factors required to evaluate it provides an interesting evaluation of the risk.

NOTE: This notion appeared in the mid-1990s within the framework of the ITSEC certification, then towards the end of this decade with the issue of global and public management of vulnerabilities and "malware" (security software vendors and CERTs). It is once again being developed at the present time with the recent release of log analysis and correlation tools that completely integrate this concept along with criticality.

severity level (of vulnerability or of nonconformity): The severity level definition is about the same as the one for incidents, with a few small differences:

- *Dangerousness*: impact of the related attacks, weakness of protective techniques, possible remote exploitation, scope of the target / victim population (number of machines, of services, …), importance to organization of the security rule that was violated.
- *Stealthiness*: same definition as for incident.
- *Exploitability* (by attackers), is the opposite definition of incident feasibility.

NOTE: The proposed definition is in line with the CVSS (NIST 800-126 [i.1] or SCAP) standard for software vulnerabilities.

security policy: overall intention and requirements as formally expressed by management

NOTE: Two levels are used: general statement and detailed rules. Rules apply to network and systems configuration, user interaction with systems and applications, and detailed processes and procedures (governance, operational teams, and audit). Violation of a rule brings about nonconformity, which is either an incident or vulnerability.

sensitivity level: level which corresponds to the potential impact (financial, legal or brand image) of a security event on an asset, an impact linked to the estimated value of the asset for the company along four possible viewpoints: its Confidentiality, Integrity and Availability (CIA) and sometimes its accountability

SIEM (Security Information and Event Management): SIEM solutions are a combination of the formerly disparate product categories of SIM (security information management) and SEM (security event management). SEM deals with real-time monitoring, correlation of events, notifications and console views. SIM provides long-term storage, analysis and reporting of log data

NOTE: The present document extends these two notions under the generic SIEM acronym, which encompasses all organizational, processes and human aspects necessary to deploy and operate these tools, and which include vulnerability and nonconformity management; it should be referred to Cyber Defence approaches in the most complex case.

taxonomy: science of identifying and naming species, and arranging them into a classification

NOTE: The field of taxonomy, sometimes referred to as "biological taxonomy", revolves around the description and use of taxonomic units, known as taxa (singular taxon). A resulting taxonomy is a particular classification ("the taxonomy of ..."), arranged in a hierarchical structure or classification scheme.

threat: potential cause of an unwanted incident, which may result in harm to a system or organization

NOTE: There are 4 categories of threats:

- Natural threats:
  - Environmental causes: public service outage, fire, and other disasters
  - System failure: physical or software computer or network breakdowns
- Human threats:
  - Unintentional (error, carelessness, irresponsibility, unawareness, etc.): conception and design, development, operation and usage, due to chance, hasty development and deployment, tiredness, gullibility, incompetence
  - Internal or external malice: theft, economic spying, sabotage, intrusion, fraud, etc.

The frontier between error, carelessness and malice is often fuzzy: it is always possible for an unscrupulous employee to plead error even though he has been negligent or malicious. However the difference between unintentional and malicious actions can often be found with the following clues:

- An unintentional action is not hidden (so not stealthy), it tends to impact availability rather than confidentiality and integrity, and it has a low dangerousness and a high feasibility. The resulting severity is often low to fairly low.
- A malicious action is stealthier (notably to enable the attacker to remain anonymous and allow him to sustain the advantages obtained for a longer period of time), with an impact on confidentiality and integrity rather than on availability, and with high dangerousness.

trace: computer data that proves the existence of a business operation

NOTE: As an example, logs (see definition elsewhere) are traces, but traces are not necessarily logs.

vulnerability: undesirable state of a system whose occurrence or detection is a security event

NOTE: It corresponds to a flaw or weakness of an asset or group of assets (at the level of a technical system, process or behaviour) that can be exploited by a threat. Occurrence and actual detection of a vulnerability (often delayed in time) are considered the same in the present document. There are 6 types of vulnerabilities, but only the first four are in the scope of a SIEM approach and are being dealt with in the present document:

- Behavioural.
- Software (that can lead to malicious exploitation by an attacker via an "exploit").
- Security equipment or software configuration (same as above).
- General security technical or organizational (vulnerabilities defined as having a global and major effect on Information System's security level, and having a level equivalent to the 133 ISO 27002 [i.7] standard reference points).
- Conception (overall system design at architecture and processes levels).
- Material level (corresponding with vulnerabilities which enable physical incidents - of an accidental, negligent or malicious kind).

A behavioural, configuration, global security (technical and organizational) or material vulnerability becomes a nonconformity (see definition above) when it violates the organization's security policy and rules. The present document uses the terms "usage or implementation drift" in this case.

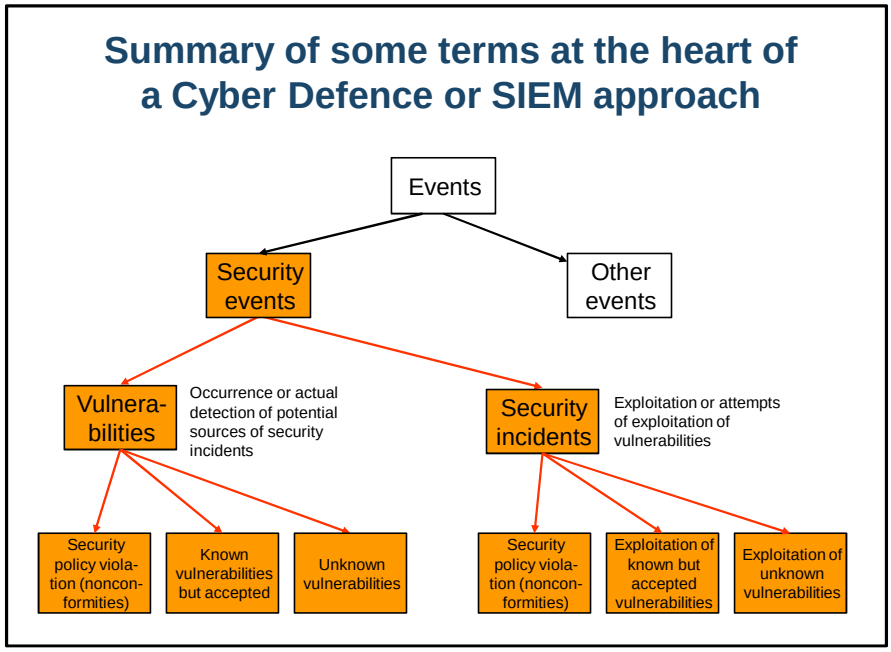

Figure 3: Relationships between different kinds of events

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AD	Active Directory
ADSL	Asymmetric Digital Subscriber Line
AMA	Advanced Management Approach
APT	Advanced Persistent Threat
ATM	Automatic (or Automated) Teller Machine
AV	Anti Virus

BYOD	Bring Your Own Device
CAG	Consensus Audit Guidelines
CAPEC	Common Attack Pattern Enumeration and Classification (Mitre)
CCE	Common Configuration Enumeration
CIA	Confidentiality Integrity Availability
CISO	Chief Information Security Officer
COBIT	Control OBjectives for Information and related Technology
CRAMM	CCTA Risk Analysis and Management Method
CSIRT	Computer Security Incident Response Team
CSS	Cross-Site Scripting (attacks)
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DAT	Digital Audio Tape
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EBIOS	Étude de Besoin et Identification des Objectifs de Sécurité
EDI	Electronic Data Interchange
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
FW	FireWall
HR	Human Resources
HTTP	HyperText Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
IAM	Identity and Access Management
ICT	Information and Communication Technology
IDB	Incident regarding Deviant internal Behaviour
IE	Internet Explorer
IEX	Incident coming from External
IMF	Incident regarding Malfunction
IODEF	Incident Object Description Exchange Format
IP	Internet Protocol
IS	Internet Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MMI	Man Machine Interface
NIST	National Institute of Standards and Technology (USA)
OS	Operating System
PABX	Private Automatic Branch eXchange
PC	Personal Computer
PDA	Personal Digital Assistant
PDCA	Plan Do Check Act
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point Of Sale
RAT	Remote Administration Tool
SAN	Storage Area Network
SANS	SysAdmin, Audit, Network, Security (SANS Institute)
SCADA	Supervisory Control And Data Acquisition
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SOC	Security Operations Centre
SP	Special Publication
SQL	Structured Query Language
SSL	Secure Sockets Layers
SSO	Single Sign-On

US	United States
USB	Universal Serial Bus (USB stick)
VBH	Vulnerability regarding Behaviour
VCF	Vulnerability regarding ConFiguration
VOR	Vulnerability with Organizational security
VPN	Virtual Private Network
VSW	Vulnerability regarding SoftWare
VTC	Vulnerability with Technical general security
WEP	Wired Equivalent Privacy
XML	Extensible Markup Language

4 Positioning of the proposed event classification model

4.1 Relationship with the ISO 27004 standard

The ISO 27004 [i.8] information security measurement model is a structure linking an information need to the relevant objects of measurement and their attributes (see Annex A for an overview of this link). The information needed generally relates to high level data used by IT security governance for decision support and improvements, whereas the objects of measurement (especially those related to technical controls) are often low level data produced by prevention and detection systems. Establishing a link between these two different worlds is easier when using an intermediate level of abstraction such as an event classification model. Building indicators consist therefore simply in counting events during intervals of constant time (see ETSI GS ISI 001-1 [i.3] and ETSI GS ISI 001-2 [i.4]).

As main outlines, the model should meet the following requirements:

- Be positioned at the appropriate level of abstraction (see clause 4.2).
- Be applicable equally to vulnerabilities and incidents (see clause 4.2).
- Include **both a taxonomy** - ensuring comprehensiveness and rigor (see clauses 4.3 and 4.4), **and a related representation model** - ensuring easy understanding and use by all stakeholders and enabling the link with indicators (see clauses 4.6, 4.7 and 4.8).
- Deal with complex security incidents represented as a combination of smaller elementary security incidents (see clause 4.5).

4.2 The critical importance of positioning the model appropriately

It is key in events and categories design and development to approach the model from the perspective of dealing with **residual or not-covered risks** hanging over the Information System. This implies that the model has to deal with the 2 components that constitute risk exposure (namely incidents and vulnerabilities, covering both detection and recovery). The model should thus be structured according to its many uses. This leads to express the two following major requirements:

- In an effort to establish state-of-the-art figures regarding the rate of incidents and of vulnerabilities, that are relevant, consistent and usable, the model main event types should be applicable to all sectors of industry, and should correspond with events aggregates that, for a large portion of them, can be understood by the current technical detection tools.
- It should be possible to associate the major types of categorized events with response and/or reaction plans (for purposes of effectiveness and of readiness).

These 2 key requirements lead to positioning the model (see diagram below) on an intermediate position between:

- The 1st position, a model that organizes and deals with the causes and reasons behind the events themselves (while explaining and notably helping with an understanding of the immense and extremely active field of malice and of the underground world that supports it).

- The 3rd position, a classification of risks closely associated with the Information System according to business lines profiles, that can be uniformly broken down into CIA risks and their associated impacts (financial, legal, image, etc.), with each risk described using a precise Top 10 (representing annual potential operational losses). This position applies only to incidents, not to vulnerabilities.

These 3 positions respectively correspond with the "who or why", the "how" and the "what and consequences" of the three (or two for vulnerabilities) previously mentioned aspects that can be used to completely describe a security event.

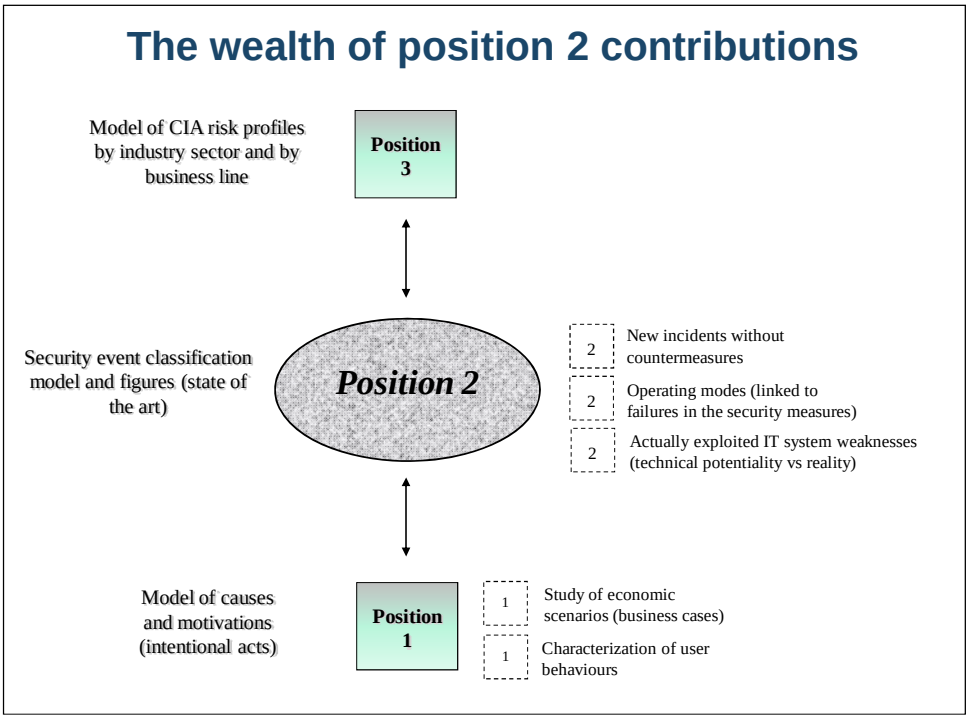

Figure 4: Positioning of the security event model

The relation between the third and the second position makes it possible to:

- Establish a very accurate link between the event classification model and the risk profiles model.
- Describe the link between the incidents categorized in the former, and the resulting disasters in the latter.
- Progressively get closer to an accurate and exhaustive knowledge of IT systems disasters (notably Confidentiality and Integrity, which are not sufficiently and accurately measured) and to an ability to quantify them for internal purposes.

The challenge for companies or organizations is thus to implement their own genuine **business-oriented IT security observatory**. Such an advanced security approach, which is focused on strategy rather than on costs, brings to light IT security aspects that impact the success or image of the corresponding business line (also influenced by the geography, the local market and the competitors). Moreover, each risk profile includes two distinct parameters (the event's frequency of occurrence and the event's impact level). Using the classification model and the related reference frameworks for indicators (and its associated statistics - see ETSI GS ISI 001-1 [i.3]) enables evaluation and benchmarking of the first parameter. The 2nd parameter is highly dependent on the sector of industry in which the IT organization operate; more mature industry sectors and/or organizations can provide sector-specific drafts and templates (notably the banking and financial world under the impetus of the Basel 2/3 AMA approach).

The relation between the first and the second position makes it possible to:

- Allow a simple link between the event model and the methods used in order to generate the events. This procedure significantly enhances the model and enables improvement of the link between the 1st position (notably malice trends) and the 2nd position (evolution of operating modes).

- Identify IT system's weaknesses that are being currently and actively exploited by attackers, which can be notably different from the ones that would in principle appear to be the most serious from a purely technical viewpoint (according to the CVSS scale, for example).
- Identify new incidents lacking immediate countermeasures.

The analysis of position three combined with the two others enables a detailed characterization of the targets selected by attackers, i.e. to highlight the preferred types of systems and/or data (for example, private data in order to support the underground world or for blackmailing, or systems to be attacked in order to disturb a country's economy insofar as possible).

Finally add that the security events included in the position 2 event model are often descriptions that can consist of a combination or sequence of elementary technical events. Each of these elementary technical events, considered on its own, does not represent an IT security event. For example, a repeatedly unsuccessful attempt to access an account becomes an IT security event only if it involves an attack focusing on the identifiers and passwords, but is not an IT security event in the case of the usual authorized user making typing errors. Elementary events are typically forwarded into logs that can be retrieved from the Information System various components, and only part of these events are later qualified as IT security events or alarms, after correlation with other elementary events or with a reference database, and very often after human and manual assessment and validation.

4.3 The necessity for the model to rest on a detailed taxonomy

To make sure that the model is exhaustive, and given that it is almost impossible to describe all possible situations, it is necessary to figure out how to define as accurately as possible security events with all the flexibility required. This leads to the definition of a detailed taxonomy (using distinct attributes for incidents and vulnerabilities), and to a complete and open dictionary of acceptable values for these attributes. With such an approach, the model needs however a way to highlight the main categories and sub-categories, to make it as understandable and usable as possible by all stakeholders. And this representation is key to acceptance by all, as explained in clause 4.6.

4.4 Description of the taxonomy

The model structure and taxonomy used to describe **incidents** is as follows (*8 areas* required to fully describe a change in a system):

1) Who and/or why (subject)
2) What (verb1)
3) How (verb 2)
4) Status of incident (attempt underway or success or failure)
5) Which vulnerability is being exploited
6) On what kind of asset (complement)
7) With what CIA consequence
8) With what kind of business impact

Each area may include up to three fields. Three areas are **mandatory** (who and/or why, what, status, asset) and the others being **optional** (how, vulnerability exploited, CIA consequence, impact).

The model structure and taxonomy used to describe **vulnerabilities** is as follows (*5 areas* required to fully describe a state):

1) What
2) On what kind of assets
3) Who (only for behavioural vulnerabilities)
4) For what purpose (only for behavioural vulnerabilities)
5) To what kind of possible exploitation

Each area may include up to 3 fields. Three areas are mandatory (what, asset, who) and the others are optional (purpose, exploitation). This description of vulnerabilities has a direct link with the NIST 800-126 [i.1] (SCAP) standard - namely CWE (Common Weakness Enumeration) - for software vulnerabilities, and the MITRE CCE (Common Configuration Enumeration) List for configuration vulnerabilities. Given the maturity and widespread use of these standards or frameworks for these 2 categories within the IT security community, the present document will only include a limited description to explain their appropriate use.

The rich information available in these descriptions (especially the cross-referencing of incidents and vulnerabilities) makes it possible to retrieve multiple results when querying a repository of detected incidents and vulnerabilities.

Annex B gives a full dictionary of possibilities for each field. The objective is to provide as many choices as possible based on diversified combinations of the different fields and on today's available state-of-the-art within the profession.

The top-level choices provided by this dictionary for incidents areas can be summarized as follows:

- *Who and/or why*: accident, unwitting or unintentional act (error), unawareness or carelessness or irresponsibility, malicious act (external or internal)
- *What*: unauthorized access to a system and/or to information, unauthorized action on the information system and/or against the organization, installation of unauthorized software programs on a system (without owner's consent), information system remote disturbance, personal or organization disturbance to induce stress, physical intrusion or illicit action, illicit activity carried out on the public Internet network (harming an organization), various human errors (administration, handling, programming, general use), breakdown or malfunction of equipment, environmental events (information system component unavailability due to a natural disaster)
- *How*: for each above-mentioned "what" possibility, list of the methods and tools used (especially for attacks)
- *Status of incident*: security event attempt underway, successful security compromise, failed security compromise
- *Vulnerability exploited*: see below the detailed description of the 6 possible types of vulnerabilities (behavioural, software, configuration, general security, conception, material)
- *Asset type*: data bases and applications (perimeter, internal, public cloud, outsourcing), systems (perimeter, internal, public cloud, outsourcing), networks and telecommunications (low level devices, high level communication, middleware, wireless devices, security), offline storage devices (paper, electronic devices, magnetic devices, optical devices), end-user devices (local application software - user or organization-owned, multipurpose-se workstations - user or organization-owned), people (employee, business partner, on-premises or off-premises service provider), facilities and environment (real estate, physical security devices or systems, various utilities, office furniture)
- *CIA consequences*: loss of confidentiality (Personal Identifiable Information (PII), trade secrets, sensitive data, intellectual property, (military)-classified material, network and systems, security), loss of integrity (many diversified cases), loss of availability (performance decrease, full breakdown or malfunction, deletion, physical destruction, physical loss including theft)
- *Impact type*: direct impact (disruption to business operations, loss of productivity, fraud, incident recovery costs, life or health consequences), indirect impact (loss of competitive advantage, reputation damage, loss of market share, legal and regulatory costs)

The top-level choices provided by this dictionary for vulnerabilities areas can be summarized as follows:

- *What:* behavioural vulnerabilities (further broken down into 10 different sub-groups), software vulnerabilities (see CWE), configuration vulnerabilities (see CCE), general security (organizational and technical) vulnerabilities, conception vulnerabilities (software, general design, environment), physical vulnerability (hardware, network and systems, personnel and site, environment)
- *On what kind of assets:* see incidents above
- *Who (only for behavioural vulnerabilities):* see incidents above
- *For what purpose (only for behavioural vulnerabilities):* see incidents above (what)
- *To what kind of possible exploitation:* see incidents above (how)

This taxonomy can be used in different ways:

- As a basis for a concise and easy-to-understand representation model to be used by all stakeholders within the organization (see clauses 4.8 and 6).
- To maintain a data base of detected incidents and vulnerabilities (according to a comprehensive and rich structure).
- To build up new organization-specific indicators based on the previously mentioned data base (different of the standard list of indicators - see ETSI GS ISI 001-1 [i.3]).
- As a rich and relevant knowledge-management tool to understand in detail the threats that need to be detected, and to configure detection tools by looking for the correct symptoms (see ETSI GS ISI 004 [i.12]).
- As an input for security event testing, to assess the effectiveness of the detection measures (see ETSI GS ISI 005 [i.13]).

Many other uses of the present event model (including the representation model) are detailed in clause 7.

4.5 Complex security incidents versus basic security incidents

One of the difficulties in describing security events (mainly security incidents) is the possible complexity of the events themselves. The present document will use the now famous example of the so-called APTs (Advanced Persistent Threats), to explain how it can be broken down in more elementary security incidents (see figure 5, with incidents represented by squares and vulnerabilities exploited by circles).

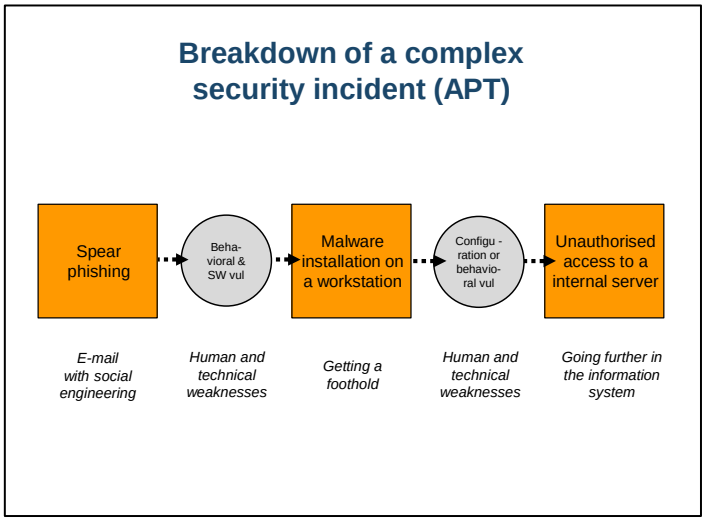

Figure 5: Description of a complex security incident

To register such a complex incident in an internal data base (for various purposes), it may be important to register each associated basic incident to gather the richest information possible on such attacks, especially:

- Know more precisely the attack vectors used (for example for malware installation, which kind of media - to be filled in the "vulnerability" field).
- In case of not fully successful attacks, know where they failed or stopped.

Other examples of (less) complex security incidents are Website defacement (intrusion followed by defacement), mis-appropriation of resources by external attackers (intrusion followed by misappropriation), backdoor on externally accessible servers acting as a foothold for future intrusions (intrusion followed by malware installation).

4.6 The key drivers underlying the representation proposed

The Club R2GS®' members' experience and feedback points out the following major factors as being decisive for a well received and successful representation. They can be summarized as follows (in ascending order of importance):

- Be simple ("elevator test" with less than one minute to explain, etc.).
- Be structured according to incidents causes and/or motivations.
- Be immediately understandable by both field IT security experts and top executives.
- Be detailed and accurate enough regarding malicious incidents.
- And last (but not the least), clearly separate internal incidents from external incidents, these two types of incidents are in almost all cases completely different, e.g. most of the internal incidents are non-technical, and sensitiveness and priorities of monitoring are quite different (see HR and social issues).

4.7 The general description of the representation

The proposed representation scheme is inspired by the one designed and used by the Club R2GS®' members, which is to date the only one to associate statistical figures with the main event types. It also builds on international advanced Cyber Defence and SIEM projects, as well as on input from academic researchers that are active in IT security research.

This representation is structured into **7 major categories** of security events. The first three categories describe security incidents that materialize threats to the Information System. The four remaining categories describe vulnerabilities and involve four of the six major types of vulnerabilities that can be exploited in order to implement an attack and create an IT security incident (see definition in clause 3.1).

The first three categories describing security incidents are as follows:

- The 1st category, called "***Intrusions and external attacks***", includes all types of incidents of a malicious nature coming from the outside.
- The 2nd category, called "***Malfunctions***", includes all types of accidental (failures or breakdowns or natural disasters) or unintentional (human error) incidents.
- The 3rd category, called ***"Deviant internal behaviours"***, includes all types of incidents of a malicious or intentional nature (negligence, recklessness and irresponsibility) originating within the company's or organization's security perimeter.

The last four categories describing vulnerabilities are as follows:

- The 1st category, called "***Behavioural vulnerabilities***", includes events which are close to some classified in the 3rd category for incidents, however without immediate CIA consequences, but where the deviant human origin of vulnerabilities needs to be pointed out.
- The 2nd category, called "***Software vulnerabilities***", includes events stemming from upstream in-house or standard software development.
- The 3rd category, called "***Configuration vulnerabilities***", includes events indicating a deviation from the accepted state-of-the-art in security policies or best practices, or a weakness which is exploited in attacks.
- The 4th category, called "***General security (technical or organizational) vulnerabilities***" includes vulnerabilities that can be defined as having an overall and significant effect on the Information System's security level and being positioned on a level equivalent with one of the ISO 27002 [i.7] standard 133 control points.

It should be added that all security events (either incidents or vulnerabilities) become non-conformities when they violate the company's or organization's security policy and rules (not including software vulnerabilities that are of a somewhat different nature).

Relative to the total incidents and based on figures gathered by the Club R2GS® (Year 2011), the various categories break down as follows:

- Intrusions and external attacks account for 52 % of the incidents observed by members of Club R2GS®, of which:
  - 2/5 involve malicious software programs (malware)
  - 3/5 for the other types of incidents
- Malfunctions account for 18 % of the incidents observed by members of Club R2GS®
- Deviant internal behaviours account for 30 % of the incidents observed by members of Club R2GS®, of which:
  - 3/4 are linked to malicious activity
  - 1/4 are linked to negligence, recklessness and irresponsibility

The proportion of malicious acts in the whole incidents database is therefore about 75 % of the total number of incidents, with the ratio between internal and external malicious acts being around 30/70 in year 2011.

Vulnerabilities (behavioural, software, configuration and general security) are involved in 80 % of the incidents of a malicious nature (see the detailed breakdown between the various types of vulnerabilities in clauses 6.4 to 6.7).

4.8 Link between the event model representation and the list of indicators (and related families)

As explained above, one of the main goals of the model representation is to provide an easy way for all stakeholders to communicate with each other, including the top governance level (ensuring that top management has access to easily understand IT security).

To identify more easily the major elements of the proposed representation, the present document proposes an organization structured in **3 levels** (categories or classes, sub-categories or sub-classes and families), associated to a naming scheme identifying categories and families (sub-categories omitted for the sake of reduction): **Category ID_Family ID** with 3 capital letters for each of Category ID and Family ID.

Moreover, given that almost all standard indicators described in ETSI GS ISI 001-1 [i.3] count numbers of security events that occurred in a given time interval, there is a **strict similarity** between the representation and the list of indicators. As a result, the naming scheme for the representation and the list of indicators will be the same. This will significantly ease the gateways between the governance level (indicator-oriented) and the field operations level (more model tied up taxonomy-oriented). These current shortcomings regarding gateways between field operations and governance are widely recognized as one of the main discrepancies in the SIEM domain.

5 Comparison with other event classification models

5.0 Introduction

Several alternative or associated classifications are currently available around the world within the framework of risk analysis and/or security objectives definition methods (EBIOS, Mehari, CRAMM, Octave, etc.), ISO reference frameworks (for example ISO 27005 [i.9]), MITRE reference frameworks (CAPEC), or recommendations within IT security communities (for example FIRST). These classifications generally cover all security incidents (and often vulnerabilities too), including hardware or software aspects, and whether they relate to breakdowns, malfunctions, human errors or malicious acts. This clause will thus compare this existing state of the art with our model, in order to benefit from their feedback and experience.

5.1 Risk analysis methods classifications

Relatively to the three positions presented in clause 4.2, the risk assessment methods classifications are positioned mostly between position 2 and position 3, sometimes on position two. From a Cyber Defence standpoint, these classifications exhibit limitations (primarily due to their objectives), in comparison with the model presented herein:

- Absence of industry-wide statistics at the level of detail of the major event categories (and sometimes impossibility to obtain consistent figures for some events since they apply only to specific industry sectors).
- Very short list of events, lacking sufficient details for widespread use, and sometimes far from the current reality of cybercrime.
- Focus sometimes primarily on incidents at the expense of vulnerabilities.
- Difficulty in establishing a link with the events described in SIEM tools used to analyse and correlate logs.
- Great difficulty to associate a consistent set of reaction plans with its various categories.

In short, these classifications are structured primarily by the "complement" and the "who" (so from the point of view of upstream risk analysis), whereas the model presented in the present document is primarily structured by the "how" and the "who" (so from the point of view of a downstream operational Cyber Defence and SIEM approach focused on detecting residual risk and reacting towards the "who" in question).

5.2 CAPEC classification

The CAPEC (Common Attack Pattern Enumeration and Classification) reference framework, which is clearly positioned on position 2, deals with the same kinds of security incidents and complements the NIST SP 800-126 [i.1] (SCAP) standard. The first CAPEC specifications were published at the end of 2007 under contract to Department of Homeland Security in the US. They have been later included by The MITRE Corporation in the complete series of Information Security Data Standards under the label "Making Security Measurable". CAPEC is a catalogue of attack patterns, along with a comprehensive classification taxonomy. By providing a standard mechanism for identifying, collecting, refining, and sharing attack patterns among the software community, CAPEC provides for a more complete and thorough review of the security level of information systems. There are however main differences with the ISG ISI approach:

- Security events are limited to malicious activity; the model does not take into account carelessness, accidents and vulnerabilities.
- The model does not include attributes related to the probability of the different types of attacks; thus the associated notion of priority is lacking, due to the absence of link to indicators and up-to-date statistical figures, so that it is not possible to emphasize the most frequent events (for example Top 50) that could make communication within an organization easier.
- As another consequence, it is impossible to extract from CAPEC a clear hierarchy and structure (for example, internal vs external attacks), and this lack of a tree structure together with an unstructured list of incidents leads to difficulties to use it on a whole organization scale.
- The lack of a top-down support finally leads to a focus on the technical description of security incidents, which is difficult to understand by non-experts.

The contribution of CAPEC to the security community is to enable understanding of the huge diversity of attack methods, thus leading to more structured approaches to develop secure software and systems, and supporting for example product certification.

5.3 FIRST classifications

The FIRST classifications [i.10] (first introduced in 2004) are being used to communicate between the CERTs and CSIRTs around the world, and they are therefore mainly focused on external security incidents. Regarding the main criteria developed in clause 4, they exhibit obvious limitations that restrict their use in a Cyber Defence and SIEM approach:

- Heterogeneous classification (see for example "Unlawful activity" and "Compromised information" categories)

- Ill-positioned model (variable depending on categories, between positions 2 and 3)
- Difficult to build a link with a structured and homogeneous reaction scheme
- Indicator-related up-to-date statistical figures impossible to collect
- Poor or missing distinction between external and internal incidents for some of them

6 Detailed description of the proposed representation of the different categories and sub-categories

6.0 Introduction

Below is a description of the proposed representation of the different categories and sub-categories (and the various families identified by the naming structure ***Category ID_Family ID***). This representation can also be considered from a **legal viewpoint**; viewing it from this related angle makes it possible to obtain accurate indications on the types of events that fall within the remit of the law, whether for the organization's benefit or detriment, and thus to obtain an estimate of the possible legal risks that organization faces. Moreover, this representation generally fits with major kinds of computer-related cases tackled today in the world by various jurisdictions.

6.1 Intrusions and external attacks (Category IEX)

Who and/or Why	What	How	Status	Which vulnerability(ies) is (are) been exploited	On what kind of asset	With what CIA consequences	With what kind of impact
Malicious act / External agent	**X** (many choices)	Only sometimes	**X** (incident attempt underway or incident success)	Only sometimes and when required for clarification	**X** (various choices)	Only sometimes and when able to be determined	-

This category includes all types of malicious security incidents originating outside of the company's or organization's security perimeter. It involves actions committed by persons unknown to company, and that are outside of its circle of existing employees, business partners, external service providers and customers. **8 sub-categories** of different security incidents gathered into **more distinct families** are identified (see summary in table 1).

Table 1

Sub-categories	Description	Comments
1	Unauthorized access to organization's information system or inter professional network	Both human motivation and use of technical means
2	Various unauthorized actions against organization's servers or applications	Both human motivation and use of technical means
3	External installation of unauthorized software programs on organization's workstations or servers	Primarily use of technical means
4	Organization's information system remote disturbance	Primarily use of technical means
5	Social engineering attacks	Primarily use of social engineering
6	Verbal act of stress	External attacker without physical action
7	Physical intrusion or action	Personal and physical intervention of attacker on an organization's technical capabilities
8	Illicit activity carried out on the public Internet, which harms an organization	External and almost out of the organization's control

1) Unauthorized access to organization's information system or interprofessional network

This sub-category includes the following families (with main types of incidents listed):

- *Family **IEX_INT*** (Technical intrusion attempt, access to a Web internal or external server via a pre-established backdoor, technical intrusion through software or configuration vulnerability on a Web server, technical intrusion on messaging accounts, illicit wireless network access, attack of VoIP protocol and internal applications, attack of a voice system - PABX mainly)
- *Family **IEX_UID*** (User's identity usurpation to get access to their account)
- *Family **IEX_RGH*** (Privileges escalation from a unauthorized access to a first usurped account)
- *Family **IEX_APT*** (Advanced Persistent Threat - A combination of several basic incidents)
- *Other families*

2) Various unauthorized actions against organization's servers or applications

This sub-category includes the following families (with main types of incidents listed):

- *Family **IEX_DFC*** (Website defacement)
- *Family **IEX_MIS*** (Misappropriation of organization on-line resources i.e. connectivity, bandwidth or storage)
- *Family **IEX_RPL*** (Transaction replay)
- *Other families*

3) External installation of unauthorized software programs on organization's workstations or servers

This sub-category includes the following family (with main types of incidents listed):

- *Family **IEX_MLW*** (Malware installation attempt, virus and worm, Trojan horse and keylogger, bot, scareware, spyware and adware, logic bomb, backdoor, RAT, etc.)

4) Organization's information system remote disturbance

This sub-category includes the following families (with main types of incidents listed):

- *Family **IEX_DOS*** (Denial of service - DoS or DDoS)
- *Family **IEX_SPM*** (Spam)
- *Other families*

5) Social engineering attacks

This sub-category includes the following families (with main types of incidents listed):

- *Family **IEX_PHI*** (Spear phishing or whaling - Cf. Usurpation of organization's acquaintance's identity to deceit a user and let him carry out a dangerous action to his organization)
- *Family **IEX_SEA*** (Baiting, elicitation, hoax/scam, etc.)
- *Family **IEX_SCA*** (Blackmail or actions meant to scare)
- *Other families*

6) Voice act of stress

This sub-category includes the following family (with main types of incidents listed):

- *Family **IEX_STR*** (Verbal act of stress from a motivated and generally unknown attacker, etc.)

7) Physical intrusion or illicit action

This sub-category includes the following family (with main types of incidents listed):

- *Family **IEX_PHY*** (Theft of laptop computers or mobile devices or removable storage devices outside the organization's perimeter, access to data of lost or stolen laptop computers or mobile devices or removable storage devices, collection of unattended documents, physical intrusion with information or equipment robbery, physical intrusion with information modification, physical intrusion with information or equipment damages, intrusion in an installed in a public place piece of equipment, eavesdropping of compromising waves, etc.)

8) Carried out on the public Internet network illicit activity, which harms an organization

This sub-category includes the following families (with main types of incidents listed):

- *Family **IEX_FGY*** (Cyber squatting or domain forgery, counterfeiting or forgery of web sites or services)
- *Family **IEX_PHM*** (Pharming)
- *Family **IEX_PHI*** (Phishing on organization's general public customers' computers)
- *Family **IEX_P2P*** (Access to protected information over P2P networks)
- *Other families*

6.2 Malfunctions (Category IMF)

Who and/or Why	What	How	Status	Which vulnera-bility(ies) is (are) been exploited	On what kind of asset	With what CIA consequences	With what kind of impact
Accident / Unwitting or unintentional act (error)	Environmental events / Breakdown or malfunction / Various errors	Only sometimes	**X** (incident occurrence underway or impact performed)	Only sometimes and when required for clarification	**X** (various choices)	Only sometimes and when able to be determined	-

This category includes all types of accidental (breakdown or natural disaster) or unintentional (human error) security incidents. This classification does not include events with an impact on people that fall into the "Health and safety" domain. The Information System taken into account is internal (managed by organization) or "external" (managed by an external service provider). **9 sub-categories** of different security incidents grouped into **more distinct families** have been identified (see summary in table 2).

Table 2

Sub-categories	Description	Comments
1	Unavailability caused by natural disaster	Cause external to organization
2	Physical failure	Accidental origin
3	Unavailability due to environmental failure	Origin stemming from a unforeseeable environmental disturbance or breakdown
4	Malfunction due to abnormal activity	Due to unforeseen deviation from normal usage patterns
5	Accidental destruction or removal of sensitive data or equipment	Due to human weaknesses
6	Accidental modification of sensitive data	Due to careless computer usage
7	Accidental leakage of protected data	Due to human error or carelessness at software development and configuration level
8	Programming error leading to system malfunction	Due to human errors or software development mistakes
9	Configuration error leading to system malfunction	Due to human errors or mistakes in system configuration

1) Unavailability caused by natural disaster

This sub-category includes the following family:

- *Family **IMF_BRE*** (Water discharge, fire, temperature effects, by a spoiling gas infection, storm, earth-quake, tidal wave, lava flow, fluid spill, equipment destruction due to an external event, etc.)

2) Physical failure

This sub-category includes the following family (same as above):

- Family **IMF_BRE** (Physical or logical cause)

3) Unavailability due to environmental failure

This sub-category includes the following family (same as above):

- *Family **IMF_BRE*** (Internal power supply blackout, external power supply blackout, air conditioning failure, by electromagnetic waves disturbance, etc.)

4) Malfunction due to abnormal activity

This sub-category includes the following family:

- Family **IMF_ANM** (On an application software connections surge, network load unusual increase, unusual server internal load, etc.)

5) Accidental removal or destruction of sensitive data or equipment (See also note at the end of clause 6.2)

This sub-category includes the following families:

- *Family **IMF_ERH*** (Manipulation or procedure error by administrators or operators during (on-line) logical files operations, data (on-line) manipulation or procedure error by administrators, procedure error by administrators during software update management, workstation manipulation error by regular users, mistake in the use of (offline) physical support devices, …)
- *Family **IMF_LOM*** (Equipment loss)

6) Accidental modification of sensitive data (See also note at the end of clause 6.2)

This sub-category includes the following families:

- *Family **IMF_ERH*** (Error by administrators during on-line files operations, by operators on-line keyboarding error, …)
- *Family **IMF_LOG*** (Shutdown of traces or log collection by administrators)

7) Accidental leakage of protected data (See also note at the end of clause 6.2)

This sub-category includes the following families:

- *Family **IMF_MDL*** (Inadvertent publication of sensitive information through voice or social networking sites or by e-mail, information leaked through a P2P exchange service due to accidental partial or full sharing of workstation resources - see possible link with incident of family ***IEX_P2P***, confidential information published on-line following a manipulation error, document loss, etc.)
- *Family **IMF_LOM*** (Equipment loss)

8) Programming error leading to system malfunction

This sub-category includes the following family:

- *Family **IMF_ERP*** (Malfunction of infrastructure components - network equipment or workstations or servers, malfunction of software products or of business applications)

9) Configuration error leading to system malfunction

This sub-category includes the following family:

- *Family **IMF_ERC*** (Misconfiguration of infrastructure components - network equipment or workstation or servers, misconfiguration of software products or business applications)

NOTE: Incidents described by these categories are often caused by careless human behaviours or poor organization's practices, but the causes of the incidents are however not tracked as a priority in this sub-category. Detailed human analysis is enabled by category 6.3. The choice of using this sub-category (or sub-category 6.2.6) or sub-category 6.3.6 for describing incidents concerning logs (key in SIEM approaches) depends on the emphasis placed by the organization on monitoring and treatment of deviant and/or possibly not compliant human behaviours.

6.3 Deviant internal behaviours (Category IDB)

Who and/or Why	What	How	Status	Which vulnera-bility(ies) is (are) been exploited	On what kind of asset	With what CIA consequences	With what kind of impact
Malicious act / Internal (employee / business partner / on-premises or off-premises service provider)	**X** (many choices)	Only sometimes	**X** (incident attempt underway or incident success)	Only sometimes and when required for clarification	**X** (various choices)	Only sometimes and when able to be determined	-

This category includes all types of security incidents of a malicious or intentional nature (negligence, recklessness and irresponsibility) originating within the company's or organization's security perimeter. It includes specifically usurpation of rights or usurpation of identity. It involves employees, business partners (including suppliers), contactors, external service providers and customers. **6 sub-categories** of different security incidents gathered into **more distinct families** are identified (see summary in table 3).

To obtain a complete view of deviant user behaviours within company or organization, it is necessary to consider another set of events, close to the present category, involving behavioural vulnerabilities (Cf. the 1st category of Vulnerabilities described in clause 6.4).

Table 3

Sub-categories	Description	Comments
1	Usurpation of identity (or user impersonation)	Either malicious action or (insane or not) curiosity or ease of use
2	Usurpation or abuse of rights (or privileges)	Wide range of cases, from strong motivation using technology to moderate information thirst-related motivation to very moderate motivation due to the sense of impunity and of all-mightiness (or to carelessness and ease of use)
3	Other sheer malicious behaviours	Generally strong motivation to enrich oneself or to harm one's organization
4	Organization disturbance	Related to the general workplace atmosphere
5	Personal attack on organization's personnel	Loss of self-control with aggressiveness level that can be extreme, or very motivated means of pressure to obtain an advantage at all costs
6	Reckless or careless action or behaviour	Deviant behaviours that can lead to critical risks

1) Usurpation of identity (or user impersonation)

This sub-category includes the following family:

- *Family **IDB_UID*** (Attempt at identity theft and/or use using technical means or social engineering techniques, illicit use of usurped identity without identity owner's knowledge and consent to access a workstation or system, use of usurped identity to deceit a given contact person, etc.)

2) Usurpation or abuse of rights (or privileges)

This sub-category includes the following families:

- *Family **IDB_RGH*** (From scratch creation of new rights, privileges escalation from existing rights using social engineering techniques, privileges escalation by exploitation of a technical vulnerability, abuse of one's privileges on a system - to access to information without any real necessity for their usual business activities and not respecting the "need-to-know", use or extension of privileges granted to a data processing specialist during field maintenance, use of groundlessly granted rights by a user, use of time-limited granted rights after the planned period)
- *Other families*

3) Distinctive sheer malicious behaviours

This sub-category includes the following families:

- *Family **IDB_IAC*** (Access to a hacking Web site from a professional workstation)
- *Family **IDB_OMB*** (Destroying action on a system or on a gateway through a professional network, groundless transaction modification or repudiation, access key theft for use on a system secured by cryptographic techniques, installation of malware on a system, social engineering attacks, abuse of company personnel abilities, physical intrusion or illicit action, etc.)
- *Family **IDB_MIS*** (Misappropriation of data processing on-line resources belonging to the organization)
- *Family **IDB_TMP*** (Access by an administrator to computer abilities to tamper with sensitive configuration data)
- *Family **IDB_UNT*** (Embezzlement or internal fraudulent action for personal enrichment or benefit, internal fraudulent action for one's organization enrichment or benefit)
- *Other families*

NOTE: This wide and disparate sub-category often does not require any prerequisite extension of privileges to carry out all possible illicit actions; illicit actions are often simply carried out by not adhering to the « need to know » principle. For example, family ***IDB_UNT*** generally relates to abuse of privileges, and more rarely appears further to an extension of rights or a user impersonation.

4) Organization disturbance

This sub-category includes the following families:

- *Family **IDB_UNR*** (Social unrest or unwarranted or excessive slowdown)
- *Family **IDB_THT*** (Threat towards an organization)
- *Other families*

5) Personal attack on organization's personnel

This sub-category includes the following families:

- *Family **IDB_STR*** (Verbal or physical attack by one user against one person belonging to the organization)
- *Family **IDB_AAC*** (Aggressive actions carried out by a manager towards a partner to obtain better sale conditions, aggressive actions carried out towards a plain user by one of their private relations to get an advantage by force)
- *Family **IDB_HAR*** (Harassment or insane repetitive actions carried out by a superior towards an employee to obtain advantages)

*6) **Reckless or careless action or behaviour***

This sub-category includes the following families:

- *Family **IDB_IUB*** (Identity illicit use to get access to a workstation or a system with identity's owner's consent and agreement, obvious use of organization's communication means for another use than by organization paid position, access to an external online service - Web, voice or news service - that is possibly harmful to one's organization, organization's storage capacity use abuse, by phone or by e-mail not encrypted sensitive data communication, on a public Web site personal data entry, misinformation or miscommunication, etc.)
- *Family **IDB_LOG*** (Shutdown of log production or storage on a system or on an application)
- *Other families*

6.4 Behavioural vulnerabilities (Category VBH)

What	On what kind of assets	Who (only for behavioural vulnerabilities)	For what purpose (only for behavioural vulnerabilities)	To what kind of possible exploitation
Behavioural vulnerabilities	**X** (various choices)	**X**	**X** (many choices)	**X** (many choices - see clauses 6.1 and sometimes 6.2 or 6.3)

This 1st category of vulnerabilities covers security events that can be attributed to a given user (developer or integrator, testing agent, system or network administrator, security administrator, computer user), and for which it is useful to stress emphasis on the human aspect of the event and to highlight the deviation from appropriate or expected behaviour (carelessness or malice); the subsequent goal is here awareness of involved users and change of associated behaviours. These events are **close to some of the previous category 6.3** (however without immediate CIA consequences for the information system), and they enable possible additional security incidents. This category can be described by identifying **10 sub-categories** of different vulnerabilities that can be gathered into **as many families** (see summary in table 4).

15 % of incidents of a malicious kind which occur in the real world have as 1st cause behavioural vulnerabilities.

Table 4

Sub-categories	Description	Comments
1	Illicit or dangerous protocols used	Great variety of situations involving low or high level communication methods
2	Internet illicitly accessed	Various dangerous methods used to prevent user tracking and escape controls
3	File illicitly transferred between the organization and the outside world	Often related to confusion between professional and private worlds
4	Workstation used without complying the required security tools, configurations and rules	Great variety of deviant practices jeopardizing workstations (widely recognized as the weakest link) and subsequently possibly the entire information system
5	Password illicitly handled or managed	Vulnerabilities remaining amongst the most frequent causes of security incidents
6	Authentication illicitly handled or managed	Can lead to very serious situations given the trust placed in such measures
7	Access rights illicitly granted	Issue to be monitored closely to avoid too many drifts damaging trust in organization overall security
8	Central systems or applications irrelevantly handled	Great variety of deviant practices concerning either administrators or plain users
9	Weakness exploited through social engineering methods	Human weaknesses exploited to make possible security incidents underway
10	Miscellaneous	All other vulnerabilities that cannot be categorized above

The description below is perfectly similar to the one of the taxonomy for behavioural vulnerabilities (see clause B.2.1.1). For this reason, only families linked to specific indicators (see ETSI GS ISI 001-1 [i.3]) are indicated here, since these ones are generally the most frequent.

1) Illicit or dangerous protocols used

This sub-category includes only one family covering all the possible viewpoints:

- *Family* ***VBH_PRC*** (Unsecured access to an Internet-facing organization-owned and managed server or application, P2P client installed on a professional workstation, VoIP client installed on a professional workstation, outbound user connection set up to get later remote access to the organization's internal network, remote or local connection to an organization's internal network from a vulnerable laptop or workstation, other unwanted or unsecure protocols)

2) Internet illicitly accessed

This sub-category includes only one family covering all the possible viewpoints:

- *Family* ***VBH_IAC*** (Internet site accessed from a professional and enterprise network by communication channels that bypass the outbound security devices, anonymization proxy used to access the Internet, etc.)

3) File illicitly transferred between the organization and the outside world

This sub-category includes only one family covering all the possible viewpoints:

- *Family* ***VBH_FTR*** (Untrusted files downloaded to a professional workstation from an external Website unknown and with no reputation within the profession, personal public instant messaging account used to exchange business files with the outside world, personal http-based messaging account used to exchange business files with the outside world, e-mail sent to an address outside of the organization with a confidential and unencrypted attachment, etc.)

4) Workstation used without complying the required security tools, configurations and rules

This sub-category includes only one family covering all the possible viewpoints:

- *Family* ***VBH_WTI*** (Professional workstation configured or accessed in administrator mode without authorization, personal storage devices - USB stick, CD-ROM, floppy, digital camera, etc. - connected to a professional workstation to exchange information or software, use of a BYOD personal device missing basic security measures intended to compartmentalize professional activities from personal ones (or use with such security measures disabled), storage of unencrypted sensitive files from a professional workstation to professional mobile or removable storage devices, presence on a professional workstation of personal software that does not comply with corporate security policy, mailbox/Internet access in administration mode, etc.)

5) Password illicitly handled or managed

This sub-category includes only one family covering all the possible viewpoints:

- *Family* ***VBH_PSW*** (Weak password used, password not changed in due time - in case of changes not periodically required, password not changed in due time by an administrator in charge of an account used automatically by systems or applications - in case of changes not periodically imposed)

6) Authentication illicitly handled or managed

This sub-category has no indicators associated (see Annex B for detailed events).

7) Access rights illicitly granted

This sub-category includes only one family:

- *Family* ***VBH_RGH*** (User right not compliant granted by an administrator outside any official procedure with malicious intent or through error or negligence)

8) Central systems or applications irrelevantly handled

This sub-category has no indicators associated (see Annex B for detailed events).

9) Weakness exploited through social engineering methods

This sub-category includes only one family covering all the possible viewpoints:

- *Family **VBH_HUW*** (Human weakness exploited by a spear phishing message meant to entice users to trigger actions that are possibly harmful to the organization - typically clicking on a public Internet link or opening an attached document, human weakness exploited through conversations (e.g. phone) leading to disclosure of secret information)

10) Miscellaneous

This sub-category has no indicators associated (see Annex B for detailed events).

6.5 Software vulnerabilities (Category VSW)

What	On what kind of assets	Who (only for behavioural vulnerabilities)	For what purpose (only for behavioural vulnerabilities)	To what kind of possible exploitation
Software vulnerabilities	**X** (various choices)	-	-	**X** (many choices - see clauses 6.1 and sometimes 6.3)

This 2nd category of vulnerabilities covers security flaws which exist in software used by organization (system or application software, acquired or developed by organization), and which can be exploited by (external or internal) attackers to carry out attacks and to trigger security incidents. This type of vulnerability is of a different kind of the 3 other types which can be detected in continuous auditing, because they are very difficult to be modified later during regular operations, due to their origin in the software development process. Moreover, these vulnerabilities are often difficult to qualify as clear nonconformities (violating software programming rules enforced within an organization).

20 % of incidents of a malicious kind which occur in the real world have as root cause software vulnerabilities.

The content of this category is extremely diversified, and no classification is proposed for this category, since a well-established and world-wide scheme exists with the CWE identification scheme (see NIST SP 800-126 Revision 2 [i.1] - Cf. SCAP). Annual surveys (such as the SANS Institute one) generally list top weaknesses categorizing them into high-level categories such as:

- Insecure interaction between components.
- Risky resource management.
- Porous defences.

Indicators associated with events belonging to this category measure the frequency of occurrence of vulnerabilities, highlighting the most common errors in application software development or patch management. For that purpose, **3 special kinds of software vulnerabilities** have been selected (representing 3 different families):

- *Family **VSW_WSR*** (Internet-facing Web applications software vulnerabilities)
- *Family **VSW_OSS*** (Internet-facing server OS software vulnerabilities)
- *Family **VSW_WBR*** (Workstation Web browser software vulnerabilities)

6.6 Configuration vulnerabilities (Category VCF)

What	On what kind of assets	Who (only for behavioural vulnerabilities)	For what purpose (only for behavioural vulnerabilities)	To what kind of possible exploitation
Configuration vulnerabilities	**X** (various choices)	-	-	**X** (many choices - see clauses 6.1 and sometimes 6.3)

This 3rd category of vulnerabilities covers events which describe equipment and software configuration errors (technical security policy not properly enforced, typical weaknesses with some configurations…), and which can be exploited by (external or internal) attackers to mount attacks and to trigger security incidents.

30 % of incidents of a malicious kind which occur in the real world have as root cause configuration vulnerabilities.

The content of this category are extremely diversified, and no classification is proposed for this category, since a well-established scheme exists with the CCE (Common Configuration Enumeration) list (see MITRE CCE Version 5 [i.2]). Standard secure configurations are available for major OS, browser, Internet server, application (Office) or cross-platform best practices. Based on these extensive lists, it is obvious to derive configuration vulnerabilities that can be also considered as non-conformities against the best current practices. Configuration vulnerabilities related to (fixed or wireless) network security (see Annex B) should be added to these lists.

Indicators associated with events belonging to this category measure the frequency of occurrence of these vulnerabilities, highlighting deviations in the application of the standard security policy by network or system administrators or shortcomings of these standard configurations. For that purpose, **9 special kinds of configuration vulnerabilities** have been selected (representing 5 different families):

- *Family* ***VCF_DIS*** (Dangerous or illicit services present on an externally accessible server)
- *Family* ***VCF_LOG*** (Insufficient storage space allocated for logs on servers or applications)
- *Family* ***VCF_FWR*** (Weak firewall filtering rules)
- *Family* ***VCF_WTI*** (Workstation wrongly configured)
- *Family* ***VCF_UAC*** (Access rights not compliant with the security policy, access rights on logs in servers which are sensitive and/or subject to regulations not compliant with the security policy, generic and shared administrator accounts that are unnecessary or accounts that are necessary but without patronage, accounts without owners - dormant or orphan accounts - that have not been erased, accounts inactive for at least 2 months that have not been disabled)

6.7 General security (technical & organizational) vulnerabilities (Category VTC and Category VOR)

What	On what kind of assets	Who (only for behavioural vulnerabilities)	For what purpose (only for behavioural vulnerabilities)	To what kind of possible exploitation
General security vulnerabilities	**X** (few choices)	-	-	**X** (many choices - see 6.1 and sometimes 6.2 or 6.3)

This 4th category of vulnerabilities covers general security vulnerabilities which are so-called for they have a global and major effect on the Information System's security level and are at the same level as the ISO 27002 [i.7] standard controls. They mostly cover the failure or malfunction of processes or of technical security tools. Indicators associated with events belonging to this category measure the assurance and effectiveness level assigned to the organization's ISMS control points, and possible occurrence of more or less important holes in "net meshes" which make up ISMS and existing security equipment and software.

12 % of incidents of a malicious kind which occur in the real world have as root cause general security vulnerabilities.

General security technical vulnerabilities are not addressed in this classification model since they do not bring sufficient added value to complement the ISO 27002 [i.7] relevant points of control. For the purpose of measurement and benchmarking, 6 special kinds of general security technical vulnerabilities have been selected (representing 6 different families):

- *Family **VTC_BKP*** (Malfunction of server-hosted sensitive data safeguards)
- *Family **VTC_IDS*** (Complete unavailability of IDS/IPS)
- *Family **VTC_WFI*** (Wi-Fi devices installed on the network without any official authorization)
- *Family **VTC_RAP*** (Remote access points used to gain unauthorized access)
- *Family **VTC_NRG*** (Devices or servers connected to the organization's network that are not registered and managed)
- *Family **VTC_PHY*** (Absence or failure of operational physical access control means and processes)

General security organizational vulnerabilities are fully addressed through a classification in main types of continuous procedure or organization control areas. This category can be described by identifying **8 sub-categories** of different vulnerabilities that can be gathered into roughly **as many families** (see summary in table 5).

Table 5

Sub-categories	Description	Comments
1	Security organization	Is the responsibility of the top security positions
2	Governance	Make sure security governance is effective and, if possible, efficient
3	Development and testing	Make sure that the initial steps in projects address IT security relevantly
4	Security operations	Directly related to continuous auditing
5	Incident detection and management process	At the core of Cyber Defence and SIEM approaches
6	Vulnerability or weakness management process	Part of Cyber Defence and SIEM approaches
7	Auditing process	Make sure auditing process is running appropriately
8	Miscellaneous	All other vulnerabilities that cannot be categorized by one of the above

The description below is similar to that of the taxonomy for general security organizational vulnerabilities (see clause B.2.1.4). For this reason, only families linked to the relevant indicators (see ETSI GS ISI 001-1 [i.3]) are indicated here, since these ones are generally the most frequently used:

1) Security organization

This sub-category has no indicators associated (see Annex B for detailed events).

2) Governance

This sub-category has no indicators associated (see Annex B for detailed events).

3) Development and testing

This sub-category includes only one family with various situations:

- *Family **VOR_PRT*** (Launch of new projects without information security classification, launch of new specific projects without risk analysis, launch of new projects of a standard type without identification of vulnerabilities and threats, launch of new projects with discrepancies identified at security level between the release of the development teams and the specification, etc.)

4) Security operations

This sub-category has no indicators associated (see Annex B for detailed events).

5) Incident detection and management process

This sub-category includes only one family with various situations:

- *Family* ***VOR_RCT*** (Reaction plans launched without feedback from previous experience, reaction plans unsuccessfully launched, etc.)

6) Vulnerability or weakness detection and management process

This sub-category includes 2 families with various situations:

- *Family* ***VOR_DSC*** (Excessive time to discovery)
- *Family* ***VOR_VNP*** (Excessive time windows of exposure due to patching mismanagement, abnormally high rate of unpatched systems for known critical software vulnerabilities, etc.)
- *Family* ***VOR_VNR*** (Abnormally high rate of rate of not reconfigured systems for known critical configuration vulnerabilities, etc.)

7) Auditing process

This sub-category has no indicators associated (see Annex B for detailed events).

8) Miscellaneous

This sub-category has no indicators associated (see Annex B for detailed events).

7 Practical uses of the event classification model

7.0 Introduction

This clause aims to demonstrate the rich and diversified uses of the event model, especially for enhanced, precise and quantitative IT security.

7.1 The classification model pivotal role

The proposed classification model is at the heart of the "Risk management / ISO 27002 [i.7] / Cyber Defence and SIEM" specification and is able to provide the central support (see clause 4 in ETSI GS ISI 001-2 [i.4]) of the implementation of such an approach. Its strength results from the various ways in which it can be used, covering the full range of topics associated with a Cyber Defence and SIEM approach. This model can therefore be used in **9 different ways**, each of which making it easier to implement a Cyber Defence and SIEM approach that is intended to be global to an organization:

- Provide input for security event testing to assess the effectiveness of the detection measures.
- Act as a gateway with the security event classifications used in risk analysis methods (more focused on "asset" and "impact" than on "what").
- Common objective to jointly evaluate the risks of potential IT security incidents on an organization's information system and their consequences on the organization itself (IT risks such as defined in risk profiles mentioned in clause 4.2).
- When implementing a Continuous Auditing scheme (notably US CAG), tracking of vulnerabilities and of the application of security-related practices, by relying on a comprehensive generic structure that deals with all kinds of security events (incidents, vulnerabilities and nonconformities), while using a common language and taxonomy.
- Detected security events that can be tied up to standard event types associated with representative public reference statistical figures (at industry sector level).
- Possible reliance for insurance companies on this public reference and on the associated metrics to define new insurance offerings for cyber-risks, and to provide new potential "insurance / security investments" tradeoffs.

- In-depth structured analysis of practices and motivations of external malicious activity as well as of abnormal or deviant internal user behaviours, including the possibility to enrich this analysis with information coming from "Counterintelligence" activity.
- Preparation of more readable reports and dashboards, with indicators directly related to certain types of very technical events that can only be managed by specialists.
- Linkage established between technical events detected by the available tools and a series of pre-defined corresponding reaction plans (with possible reliance on a reference framework in this domain).

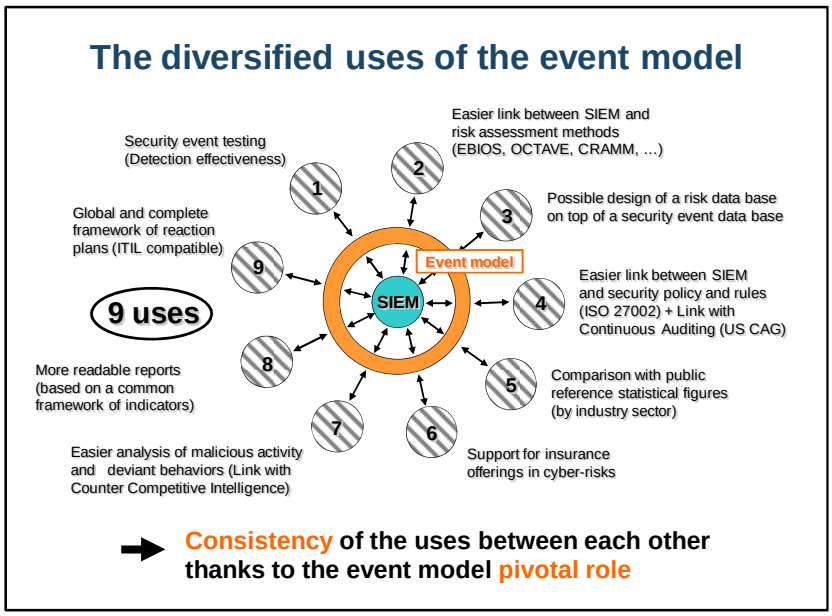

Figure 6: Different use cases of the security event model

The classification model pivotal role is clearly obvious here, and figure 6 shows its impact on the **9 usages**, notably thanks to the model being structured at the right abstraction level, and to the pedagogical and cross-functional orientation of its categories and components.

The next 3 clauses provide a more detailed analysis of several uses of the model, with a particular focus on correspondence with risks (clause 7.2) and all possible links with the work carried out around the world on the issue of cybercrime and its motivations clause 7.3).

7.2 The objective shared with operational risks

This clause clarifies and provides further information to the introduction of this subject in clause 4.2. While the proposed classification model is universal and common to all industry sectors, the operational risks modelling (on the 3rd position) is only doable when applied to a specific industry sector. By reviewing the work carried out on this level, is realized the relevance and validity of such an approach, provided that it can be identified the true root business lines that constitute the "industry sector", and thereby derive the right risk profiles. Once this work has been done, each company or organization in a given industry sector can then deduce a hierarchy of its own risks, by combining the various standard risk profiles with specific, locally-defined weights. The maturity of such an approach is highly dependent on the industry sector:

- The banking and financial sector is the most advanced one thanks to the drive provided by the implementation of the Basel 2/3 advanced approach for operational risks, and to its objective of better risk control.
- A few other industry sectors seem to be interested in this kind of modelling and approach, and specific efforts have been undertaken, though they remain generally isolated and restricted to specific companies or organizations (primarily American). This is the case of the telecommunications sector, the utilities sector, the airline transportation sector, the postal sector, and certain large sensitive administrations (Defence, for example).

- The remaining industry sectors view such modelling as less essential, for several reasons: the number of business lines and of risk profiles within a given company are limited to one (instead of more than 20 in some of the aforementioned sectors), the share of (computerized or not) IT-related operational risks is much smaller (up to 70 % in some of the aforementioned sectors), and they are less mature with respect to IT security.

The link between position 2 and position 3 is such that for each identified operational risk, there can be one or more unambiguously associated events coming from the model. Experience has shown that the present document statistically covers more than 99 % of security events occurring in the real world.

7.3 The link with existing studies on cybercrime motivation (threat intelligence)

This clause develops the 1st modelling position and its linkage with the 2nd position classification model. While the 2nd and 3rd positions can be precisely described, formalized and operationally implemented in many companies or organizations, the 1st position does not currently seem to link, to our knowledge, to reference frameworks that are as well established and disseminated as the aforementioned ones. If are set aside the causes consisting of breakdowns and human errors (generally well-known) and while concentrating on malicious activity, several interesting (public) studies in the cybercrime area provide documented starting points for further thought:

- The "Report on the Underground Economy", periodically published by Symantec® (external malicious activity).
- The "Online Fraud" report, periodically published by RSA® (external malicious activity).
- The report entitled "The Big Picture of Insider IT Sabotage Across US Critical Infrastructures", published by the Software Engineering Institute of the American Carnegie Mellon university (internal malicious activity).

Positioned on the 1st position, these studies are carried out from the point of view of the **"Offensive Cyber Security"**, in comparison with the "Defensive Cyber Security" vision that relates to the 2nd and 3rd positions and is the primary focus of the present document up to this point. Indeed, these studies (from Universities or public/private Observatories) analyse motivations, modus operandi and quantified trends in terms of external or internal malicious activity (with the latter seemingly having been less explored).

The major types of cybercrime can be categorized as follows:

- State espionage.
- State or Government-related ("militia") cyber-attacks.
- Terrorism-related cyber-attacks.
- Large-scale organized criminal fraud (through theft or not of personal identifiable information, and thanks to a developed underground economy that is becoming increasingly specialized).
- Making justice oneself (e.g. little organized groups such as Anonymous, wishing to make public knowledge negative behaviours as regards some organizations).
- Business intelligence in companies (theft of confidential information or disruption of competitors).
- Sabotage or dangerous individual behaviour against an organization (due to a strong need for recognition).
- Individual fraud targeting an organization (motivated, planned and resorting of significant means).
- Individual fraud against one's employer's organization (opportunistic).
- Individual retaliation or revenge against one's employer's organization (after harsh and unfair treatment by the latter).
- Access to confidential information by extreme curiosity.
- Individual attacks for fun or for personal glory (script kiddies).

These 12 categories can be carried out whether inside or outside an organization, with or without the help from an organization's employee. They can also be grouped into 5 major groups: States (1), terrorism and crime (2), self-administered justice (3), companies (4), isolated individuals (5). The respective origins of actions for each of these groups are the following:

- Desire of a sovereign state to control its security and safety.
- Terrorism of any type (e.g. intrusion into SCADA-type critical infrastructures in order to cause a shutdown), and appetizing new revenue sources for crime.
- Self-administered justice (e.g. little organized groups such as Anonymous, wishing to make public knowledge negative behaviours by specific organizations).
- Desire to increase the company's productivity, by accessing and using its competitors' confidential data or by disturbing their activity (Website and image, for example).
- Individual interests (greed, spirit of revenge, pride, need for domination, need for recognition, intense curiosity, fear, etc.).

Each of these 5 groups has its own rationale, and can only be fought with a precise idea of the underlying motivation levels, of the potential technical means available to attackers, and of the frequency of occurrence of attacks that can typically be expected; on this latter point, it is for example possible to rely on the statistical predictability of human behaviour: for example, studies show that 95 % of individuals would opportunistically yield to the temptation to steal hardware whether an opportunity arises unexpectedly while offering little danger for them, and that 90 % of individuals experience a feeling of resentment when victim of unfair actions that will strongly impact their lives (dismissals, for example). In the attackers' modus operandi, it is also necessary to consider the fact that resorting to **social engineering** has sharply increased recently, and that a majority of attacks rely, at least partially, on the exploitation of human weaknesses. This finding (that partly comes out in several studies) should push companies and organizations to enhance and focus awareness-raising actions for their employees. Finally, let us mention the common feature of all types of malicious activity, namely the craving and pleasure that are felt when breaking rules and codes laid down by a company, both of which are powerful factors behind them.

At this point, it is important to return to the statistical aspects linked to malicious activity, briefly mentioned in clause 4.7, and to give some additional figures that illustrate the above statements (figures also coming from Club R2GS®). First of all, it is mandatory to stipulate that about 75 % of all currently occurring security incidents stem from malice and aggressive behaviour. The following figures highlight a few striking trends of external attacks (% relative to all security incidents, excluding failed attempts):

- 0,1 % of incidents involve DoS or DDoS attacks; this figure has risen sharply and that can primarily be related back to 2 groups:
  - Group 1 regarding "militia" attacks that seem to occur more or less regularly here and there around the world alongside local political or military crises, or nationalist demonstrations relative to one foreign country or another.
  - Group 5 regarding individual initiatives, with demonstration of a genuine power to be a hindrance (most frequent case), or retaliation against sites accused of unfair practices, or execution of threats in order to get ransom.
- 3,5 % of incidents involve intrusions into public Websites; these attacks also are clearly increasing - with a particular focus in the USA - and are primarily tied up to group 2. The aim is usually to directly steal personal identifiable information from the site itself, or to corrupt Web pages for the subsequent purpose of installing malware on the workstations of users connecting to the site, once again with the ultimate aim to steal personal identifiable information. Such personal identifiable information is then sold on an organized "underground" market, and/or used directly in order to perpetrate bank fraud (money transfers from hacked bank accounts to offshore accounts, followed by transformation into cash).
- 1 % of incidents involve public Web sites defacement; these events also show a clear increase and are associated primarily to 3 groups:
  - Group 1 regarding "militia" attacks, with the same motivations as for DoS or DDoS attacks.
  - Group 4 regarding objectives for a company to alter the image of its competitors.

- Group 5 regarding sabotage or dangerous behaviour against an organization, out of a strong need for recognition.

- 21 % of incidents involve the installation of malware on companies' or organizations' workstations and servers. This figure has shown the strongest increase in the last years (all incidents taken together), and can primarily be associated to 3 groups:
  - Group 2 regarding installation of bots in order to establish huge botnets that can be used for various purposes by criminals.
  - Group 3 regarding detection and evidence gathering of malicious behaviours.
  - Group 4 regarding espionage involving sensitive industries and administrations, which can also involve States - Cf. increasingly more spear phishing.

The following figures highlight aspects of internal attacks that deserve particular attention (% relative to all incidents, excluding attempts):

- 1 % involve only identity theft. This figure has been quite stable in the last two years, which can primarily be tied up to group 5. They mainly originate from exaggerated curiosity to obtain confidential data about managers or directors or individual customers (most often), or simple curiosity regarding internally hidden information.

- 0,5 % involve abuses of privileges by administrators or developers. This figure has seen some increase in recent years, and that can be associated primarily to group 5. Their main origins are exaggerated curiosity to obtain confidential data about managers or directors or individual customers (most often), or greed or desire for personal glory through misappropriation of IT resources in order to build and operate Internet sites or to be able to carry out downloads to associations that use P2P to distribute files (music, films, etc.).

- 0,8 % involve user's illicit usage of privileges that remain active after leaving his position within the organization. This figure has stabilized somewhat in recent years (notably thanks to IAM approaches). The incidents can primarily be associated to group 5. They primarily originate from exaggerated curiosity to see if it still possible to enter one's former department or organization, or quite simply from the perpetuation of past habits (case of an internal transfer without leaving the organization). Serious cases can also arise with access to and destruction of files, the motive coming from resentment and revenge against the old organization with whom the separation has gone very badly; less frequent but still at quite a high rate (1 %) in view of their possible consequences, these cases have been increasing steadily in the last 10 years and should be therefore a subject of particular attention for organizations.

The various noteworthy examples, of both external and internal origin, demonstrate the interest and value of being able to link position 1 cybercrime behaviour and motivation analyses with the position 2 classification model's major types of events (and their associated statistics). In some ways, the aim is to give qualitative approaches (which can be very extensive) an additional quantitative dimension that will allow for a precise measurement of the phenomena and of the power of the methods implemented in order to remedy or decrease them.

Another complementary approach angle for cybercrime consists of the **study of economic scenarios** (i.e. business cases) for each main threat type, while relying on a balance sheet "(organization or individual) costs and risks versus opportunities for gain" analysis; this can notably help to better understand why some attacks occur rarely, and others very often. The risks to be taken into account vary greatly, and can involve:

- For a State (group 1), damage to its relations with other countries or to its international image.

- For a criminal organization (group 2), difficulty in monetizing some types of information on the "underground" market and attacks by rivalling organizations disturbed by its activities (attacks that could disturb a complete network of bots for example).

- For these individuals or organizations (group 3), potential financial and legal consequences.

- For a company (group 4), potential legal consequences, or ones affecting its image or its business in case of detection of the attack's exact origin.

- For an individual (group 5), potential personal consequences in legal and financial terms (in case of conviction), as well as to one's professional image and therefore "employability" in the future. In this group however, an analysis of this type can prove difficult, given the often very irrational nature of the potential behaviour types.

7.4 The link with incident exchange

Indicators may need to be shared by the organization that manages them, or to be consolidated inside organizations. For this purpose, there is a need for a representative format. The present document suggests and illustrates the use of the Incident Object Description Exchange Format (IODEF) maintained by the Internet Engineering Task Force. The present document uses the new version (version 2) of the format currently being revised by the IETF, and more specifically version -11 of the format (draft-ietf-mile-rfc5070-bis-11 [i.6]) dated March 23rd, 2015. While there may be modifications to the standard after this date, the current format is stable enough to be included here; however, since there have been changes from 1.0 related to indicators information, the use of the IODEF 2.0 specification is required.

Rationale

IODEF is a format for exchanging information between CERTs. Several SIEM platforms are also considering the use of IODEF to export and exchange incident information. In particular, the IODEF standard aims at enabling cyber-information meta-data sharing and interoperability, which are common goals with the present document. Within the realm of the present document, the IODEF data model includes several notions that are of interest:

- Incident: an IODEF message is necessarily an incident. Since indicators are information that qualify a particular set of incidents, they constitute an incident by themselves that needs to be communicated.

- IndicatorClass: The IODEF standards includes the capability to formulate indicators natively. This structure fits the purpose of the present document well, particularly since it includes the capability to link indicator information over time or hierarchically.

- Restrictions: the IODEF standard includes the ability to attach restrictions of transmission to documents. This is important for organizations that need to control the diffusion of information.

- Threat information (campaigns, threat actors, etc.): the IODEF standard includes the capability to represent many if not all types of incidents that can affect an organization. Thus, detailed sharing of information associated with indicators is also available.

As a summary, the IODEF standard includes all the necessary support for indicator information exchange.

Implementation recommendations

Using the IODEF standard format to share ETSI ISI indicators should follow these recommendations (Omitting the outer envelope IODEF-Document for the sake of simplicity) :

- IODEF-Document: an IODEF-Document should be created any time an indicator is generated. The IODEF-Document.version should be 2.00. The IODEF-Document.formatid should convey the information that the document contains ETSI ISI indicators. The IODEF-Document should contain at least one Incident describing at least one indicator.

- Incident: each indicator should be described within an IODEF-Document.Incident sub-document. If several indicators need to be transmitted, then each indicator should be described in a separate IODEF-Document.Incident subsection, or in a separate IODEF-Document.Incident.IndicatorClass.Indicator subsection. The former practice is recommended for unrelated indicators (i.e. indicators belonging to different categories IEX, IMF, IDB, VBH, WSW, VCF, VTC, VOR). The later practice is recommended for indicators belonging to the same category (e.g. VTC_IDS, WTC_WFI and VTC_MOF):

    - Incident.purpose should be set to 3 (reporting), to indicate that the IODEF-Document has been sent to comply with reporting purposes.

    - Incident.restriction should be adapted for the needs of the organization. By default, the restriction is set to 4 (private), indicating that the information should not be shared.

- Each message should be assigned a unique Incident.IncidentID identifier; in the context of the present document, this IncidentID should be new for every computation of the indicator. The Incident.IncidentID.name should identify the component or entity in the organization generating the message. This could be a person, an organizational entity, or a software platform.

- Incident.ReportTime: the timestamp of the moment the IODEF-Document is sent. This is the only mandatory timestamp. For the sake of simplicity, the present document recommends that the Incident.GenerationTime records the time at which the indicator is computed. If the indicator covers a known time period, the present document recommends that the Incident.StartTime and Incident.EndTime are left empty, this information being carried in the Indicator subsection.

- Incident.RelatedActivity: if the present document is used to implement cascaded indicators, then this class should be used to refer to the original sub-indicators.

- Incident.Assessment: if the indicators associated with the present document are used to compute the impact of attacks on the organization, then this class should be used to describe the impact.

- Incident.HistoryItem: if the indicators associated with the present document lead to actions that should improve them, then this class should be used to trace the actions taken.

- Incident.IndicatorData: this class should contain the actual information about the indicator. It is associated with one or several “Indicator” sub-sections.

- Incident.IndicatorData.Indicator: each of these subsections should describe a single indicator.

    - IndicatorID: this identifies the Indicator. The complete identification of the indicator should be used. The present document recommends the use of the following form: “ETSI:ISI:indicator-category_indicator-family”. (e.g. “ETSI:ISI:VTC_IDS”)

    - Description: this is a textual message associated with the indicator. The operator, entity or platform generating the indicator may indicate additional information related to the implementation of the indicator.

    - StartTime: If the indicator covers a known time period, then the present document recommends that this value contains the timestamp of the beginning of the period over which the indicator is computed.

    - EndTime: If the indicator covers a known time period, then the present document recommends that this value contains the timestamp of the end of the period over which the indicator is computed.

    - Contact: if the person, entity or platform generating the indicator is known, then the present document recommends that it is identified in the Contact information.

    - Observable: This class is used to carry the actual value of the indicator. This value should be stored in the Observable.RecordData.RecordItem sub-section, indicating the type (integer, real, etc) in the attributes and the value as a final element).

EXAMPLE:

The following IODEF message describes the encoding of a VTC_IDS indicator, reporting a 12 % unavailability over the last 24 hours.

```
<?xml version="1.0" encoding="UTF-8"?>
<IODEF-Document version="2.00" lang="en"
xmlns="urn:ietf:params:xml:ns:iodef-1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:schema:iodef-1.0">
<Incident purpose="reporting">
   <IncidentID name="org.example.com">189493</IncidentID>
   <ReportTime>2015-01-13T23:19:24+00:00</ReportTime>
   <Description>Indicator VTC_IDS</Description>
      <IndicatorData>
         <Indicator>
            <IndicatorID name="org.example.com">ETSI:ISI:VTC_IDS</IndicatorID>
            <StartTime>2015-01-12T12:00:00+01:00</StartTime>
            <EndTime>2015-01-13T12:00:00+01:00</EndTime>
            <Observable>
```

```
            <RecordData>
               <RecordItem dtype=”Integer”
                  meaning=”percentage of unavailability of IDS sensors during the
               period”
                  formatid=”percentage”>12</RecordItem>
            </RecordData>
         </Observable>
      <Indicator>
    </IndicatorData>
  </IncidentID
</Incident>
</IODEF-Document>
```

7.5 Other uses of the classification model

Alongside these 2 uses, 7 other uses of such a model are currently seen or foreseeable in time:

- Security event testing: the model (especially the taxonomy) is a basic input to produce security events, test and assess consequently the effectiveness of the detection measures. Testing and performance evaluation are key to improve the credibility and RoI (Return on Investment) by improving dramatically the event detection rates that are today so low for so many types of events. The ability to provide a solid ground for precise testing scenarios for a typical set of security events is therefore of utmost importance to measure the systems and tools performance.

- Risk analysis methods: the aim is to extract general results from the risk analysis undertaken for specific individual systems, while refining the residual risk contents that is updated by means of the model event types and associated lists. A progressive enhancement of the classifications currently proposed within the risk analysis methods could eventually lead to their replacement by this model (as can be seen in the USA with Octave).

- Continuous Auditing (ISO 27002 [i.7] or US CAG or possibly COBIT - see ETSI GS ISI 001-2 [i.4] for details): the contribution of the model is either to help with the definition of a series of control points where no control of this type had previously existed, or to refine and optimize existing controls. In all cases, the core value of the model is the overall consistency with other concomitant usages (such as an organized reaction scheme or benchmarking through indicators), and the possibility of defining a precise implementation of these 2 uses by means of an organizational interface between the monitored system and the possible central SOC in charge of this monitoring. Such a strictly formalized interface can contribute to progress and to the following clarifications:

  - Accurate definition of residual risk taken into account (vulnerability x threat x impact), while identifying priority 1 action levers.

  - Prioritized list of events (incidents, vulnerabilities, nonconformities) on the IT system that is monitored within the framework of an internal service contract, while relying on the classification model.

  - Precise evaluation of event criticality (event severity x impacted target sensitivity).

  - Thorough identification of the people involved in the security chain (security managers or correspondents on various levels, network or system administrators, operational owners or managers of the monitored IT system components, etc.), and their exact role as part of handling such events.

  - List of standard reaction plan types that have to be launched (while relying on an existing reference framework - see below).

  - Organization of escalation and of crisis management structures in case of non-standard events and ones not categorized as critical and/or ones that escape the SOC's control.

  - Definition of the expected SLA-type service levels (time for notification, qualification, recommendation of solution, event resolution, etc.).

- Use of metrics shared by professionals: the model provides an event classification at the right level (as determined in a convergent manner within a series of advanced SIEM projects), which makes it possible to produce a truly objective benchmarking of organization's security level via some relevant operational indicators and the establishment of a corresponding state-of-the-art.

- Based on this state-of-the-art and on the associated metrics, a 4th additional use is related to the definition by insurance companies of new insurance policies and associated premiums for cyber-risks. The aim here is to design and verify the relevance of new "insurance / security investments" trade-offs while covering, for example, increasing risks related to cybercrime; typical examples are DDoS attacks (occurring very randomly and irregularly within organizations, but with few prevention means and consequences that can be significant in terms of image) or internal fraud committed by employees or external service providers (somewhat more predictable occurrence frequency than the previous event, but also with prevention means and technical and procedural controls that cannot eliminate all risks, and financial consequences that can be considerable). Such events lend themselves well to the insurance notion, and thus to the pooling of risks within a profession.

- The 5th additional usage involves the definition of operational indicators for incidents and vulnerabilities / non-conformities extracted from the ones which can be associated with a state-of-the-art. This involves relying on the classification model and its major event types (in principle, extensively disseminated and known within company or organization), preparing simpler and more readable reports and dashboards with indicators that are often innovative and also directly related to some types of very technical events that can only be grasped by specialists; for this purpose, it is also possible to rely on an existing reference framework.

- The 6th and last additional use relates to the possibility of associating, with many types of categorized events, standard reaction plans that are intended to deal with these events and to come back to a normal situation. To that end, it is better to rely on an existing reference framework, which typically includes some 30 standard plans generally organized into 5 strictly formalized steps. Experience has shown they would manage to cover, within the best international SIEM projects, nearly 95 % of the events occurring in the real world, and that more than 90 % of the launched plans were efficient for solving the problems resulting from events.

Annex A (informative): Overview of the ISO 27004 standard measurement model

The ISO 27004 [i.8] information security measurement model is a structure linking an information need to the relevant objects of measurement and their attributes. Figure A.1 (© ISO/IEC 27004:2009 [i.8]) depicts this model. And the event classification model (the present document, ETSI GS ISI 002) and the related list of events counted (derived measures of ETSI GS ISI 001-1 [i.3]) are positioned against it.

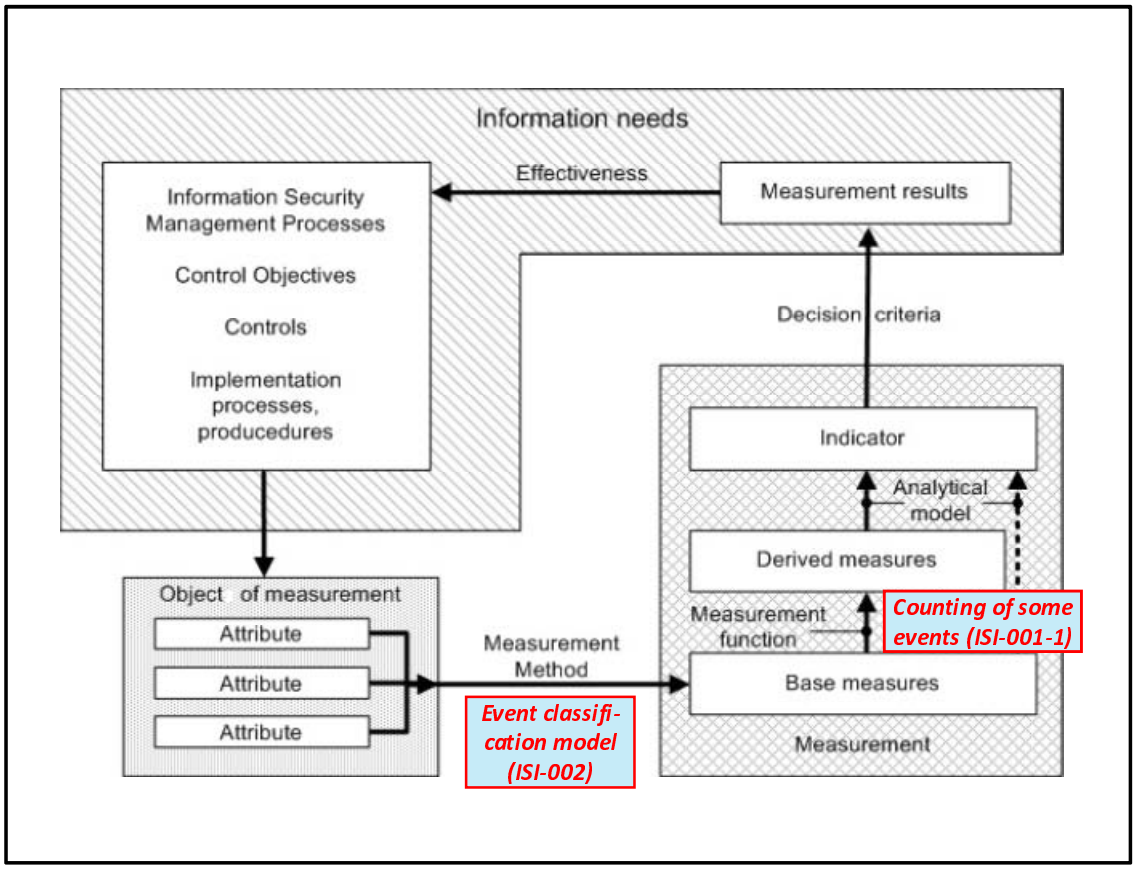

Figure A.1: ETSI GS ISI 001 [i.3], [i.4] and ISI 002 positioned against ISO 27004 [i.8]

Annex B (informative): Field dictionary for the taxonomy

B.0 Introduction

It should be mentioned here that the following lists are not exhaustive although they should be considered as almost comprehensive.

B.1 Incidents

B.1.1 Who and/or Why

B.1.1.1 Accident

1) Natural disaster
2) Physical failure
3) IS environment component unavailability
4) Software malfunction: development, implementation
5) Abnormal activity

B.1.1.2 Unwitting or unintentional act (error)

1) Internal (employee):
   - Administrator
   - Maintenance
   - Operator
   - Software developer
   - Manager
   - Executive
   - End-user
   - Other
2) Internal (on-premises or off-premises service provider):
   - Administrator
   - Maintenance
   - Operator
   - Manager
   - Software developer
   - Other

B.1.1.3 Unawareness or carelessness or irresponsibility

1) Internal (employee):
   - Administrator
   - Maintenance
   - Operator
   - Software developer
   - Manager
   - Executive
   - End-user
   - Other
2) Internal (on-premises or off-premises service provider):
   - Administrator
   - Maintenance
   - Operator
   - Manager
   - Software developer
   - Other

B.1.1.4 Malicious act

1) External agent:
   - State or government
   - Militia (government-related)
   - Terrorism
   - Organized crime group
   - Activist group
   - Corporation
   - Individual person (revenge against the organization)
   - Individual person (fraud)
   - Individual person (fun or personal glory - Cf. script kiddies)
   - Individual person (insane curiosity)
2) Internal (employee):
   - Administrator
   - Maintenance
   - Operator
   - Software developer

- Manager
- Executive
- End-user
- Other

3) Internal (business partner):
   - Supplier
   - Reseller or distributor
   - End-user customer
4) Internal (on-premises or off-premises service provider):
   - Administrator
   - Maintenance
   - Operator
   - Manager
   - Software developer
   - Other

B.1.2 What

B.1.2.1 Unauthorized access to a system and/or to information

1) Use of authorized user's identity (identity usurpation or user impersonation): with or without identity owner's consent and agreement
2) Access to a network or a central system or an application via a pre-established foothold (for example back-door)
3) Technical intrusion on a network or a (central or end-user) system or an application
4) Intrusion on a central system or an application via a stolen (or lost) and ill-protected workstation having access to organization's internal network through a VPN connection
5) Usurpation of rights:
   - From scratch creation of new rights
   - Privileges escalation
   - Legitimately granted rights used and exploited in an uncommon (or illogical) and illicit manner (abuse of rights and lack of respect of the "need-to-know")
   - Illicit use of left privileges after leaving an organization or changing position within the organization
   - Illicit use of rights granted without any reason
   - Use or extension of rights granted to a computer specialist for a field intervention
   - Use of time-limited granted rights after the planned period

6) Other

NOTE 1: "Into electronic communication coming" is included either in clause B.1.2.3, 2) (communication interception through sniffing) or in clauses B.1.2.1, 1), B.1.2.1, 2) or B.1.2.1, 3) (attack of VoIP protocol/commanding and private application software) or in clauses B.1.2.1, 6) (attack of vintage voice system so-called war-dialling) or B.1.2.7, 3) (wiretapping).

NOTE 2: "Illicit wireless network access on an unprotected or poorly protected internal network" is included in clauses B.1.2.1, 1), B.1.2.1, 2) or B.1.2.1, 3).

B.1.2.2 Unauthorized action on the information system and/or against the organization

1) Website defacement

2) Misappropriation of organization on-line resources i.e. connectivity, bandwidth or storage

3) On a system or on a gateway towards a professional network destroying or disturbing action

4) Obvious use of organization's communication means for another use than the one paid for by the organization (or excessive non-business use)

5) Access from a professional workstation to an external online service (Web, voice or news service) that is possibly harmful to one's organization (mainly loss of productivity or unlawful content access or heavy overhead or further malicious activity enabled):

   - Hacking public Web site
   - Public Website (that has no relation with one's professional activities)
   - Public Website (that has some relation with his/her professional activities, but in violation of one's employment contract)
   - Internal user's access to unknown vocal sites after solicitation by SMS (SMishing)
   - Internal user's access to unknown vocal sites after receiving a telephone call (Vishing)
   - Other

6) Storage of inappropriate content in a PC

7) By phone or by e-mail (not encrypted) sensitive data communication

8) On a public Web site personal data entry

9) Shutdown of log production and/or storage on a system or on an application

10) Internal fraudulent action for personal enrichment or benefit: through computer or not (embezzlement)

11) Internal fraudulent action for one's organization enrichment or benefit: through computer or not (for example

12) External fraudulent action on a VoIP or not voice system:

   - Telephone capacity misappropriation
   - Artificial traffic increase in order to increase billing

13) Groundless transaction modification or repudiation: concerns business partners (customers, distributors and suppliers)

14) Transaction replay

15) Communication or message or file decryption

16) Access key illicit robbery for use on a system secured by cryptographic techniques (concerns typically PKI systems and private keys)

17) Company member abilities abuse:

- At company's corporate assets level power abuse
- Confidence abuse

18) Miscommunication or misinformation: transmission of false information to a user by another one

19) Other

B.1.2.3 Installation of unauthorized software programs (malware) on a system (without the owner's consent)

1) Virus and worm (disturbing and visible due to propagation features, meant to harm the information system). C&C (Command and Control) channel are not used

2) Trojan horse and keylogger (generally stealthy, meant to steal information or sent commands or attacks to other internal systems, but propagation features may be also available as above). C&C channel are used and necessary

3) Bot (generally stealthy, meant to launch attacks outside the organization, such as DDoS, spam, etc. but propagation features may be also available as above). C&C channel are used and necessary

4) Scareware (installed on a workstation and meant to scare and entice the user to purchase an antivirus program that may be a malware itself). C&C channel are used and necessary

5) Spyware and adware (only on workstations). C&C channel may be used

6) Other (logic bomb, backdoor, RAT, etc.)

B.1.2.4 Information system remote disturbance

1) Denial of service (DoS or DDoS)

2) Disturbance of messaging system regular operations:

- Spam reception
- Reception or sending of very oversized messages or attached pieces

3) Other

B.1.2.5 Social engineering attacks

1) Usurpation of organization's acquaintance's identity to deceit a user and induce him to carry out an action dangerous to her organization:

- Attempt to deceit a user through a spoofed and customized e-mail faking a known authority or business relation (spear phishing or whaling, generally the starting point and preferred mean of APTs)
- Deception on the phone of an organization's call centre operator
- Deception of mobile phone users

2) Baiting (scattering infected media such as USB sticks in parking lot)

3) Blackmail or actions meant to scare:

- Funds extortion attempt by threatening retaliation against an organization, using technical means (ransomware)
- Actions meant to scare (through scareware)

4) Elicitation (subtle extraction of information through conversation)

5) Hoax/scam

6) Other

B.1.2.6 Personal attack on organization's personnel or organization disturbance

1) Personal attack on organization's personnel:

   - Voice or physical attack by one person against one person belonging to the organization
   - Aggressive actions carried out by a manager towards a partner to obtain better sale conditions
   - Aggressive actions carried out towards a plain user by one their private relations to get an advantage by force

2) Personal harassment:

   - Unacceptable repetitive actions carried out by a superior towards an employee to obtain advantages

3) Organization disturbance:

   - Social unrest or unwarranted or excessive slowdown (including strike)
   - Towards one's organization clear case of threat

B.1.2.7 Physical intrusion or illicit action

1) Access to data on a lost or stolen laptop, workstation, mobile device or removable storage device (theft outside organization)

2) Collection of unattended documents

3) Physical intrusion resulting in theft of information or equipment: illicit access to protected perimeter or premises to steal equipment or information (directly - via local interface or via local connection of workstation-like device on the network - or indirectly through wiretapping)

4) Physical intrusion resulting in information modification: illicit access to protected perimeter or premises to modify information (directly via local interface or through implementation of a switch device to tamper and sent again the data received)

5) Physical intrusion resulting in information or equipment damages: illicit access to an organization owned asset to damage or destroy sensitive information or equipment (sabotage)

6) Intrusion in a piece of equipment installed in a public place:

   - Vandalism or material damages
   - Information theft

7) Eavesdropping of radio waves: workstations, telephone handsets

B.1.2.8 Illicit activity carried out on the public Internet (harming an organization)

1) Cybersquatting or domain forgery

2) Pharming

3) Counterfeiting or forgery of Web sites and/or services (mainly to develop forged business or for phishing purposes)

4) Phishing (targeting organization's general public customers' computers)

5) Spreading false or secret information about an organization through unmoderated social networking

6) Access to protected data over P2P networks

7) Other

B.1.2.9 Various errors (administration, handling, programming, general use)

1) Accidental removal or destruction of equipment or sensitive data:

   - Manipulation or procedure error by administrators or operators during (on-line) logical files operations (relates to destruction of living or archived data)
   - Data (on-line) manipulation or procedure error by administrators (relates to modification of data making them unusable)
   - Procedure error by administrators during software update management (relates to information loss)
   - Workstation manipulation error by regular users (relates to information loss or destruction)
   - Mistake in the use of (offline) physical support devices (relates to mislaying of all kinds of information supports, whether computerized or not)
   - Equipment loss (concerns especially laptop workstations or mobile devices or removable storage devices)
   - Other

2) Accidental modification of sensitive data:

   - Error by administrators during on-line files operations (relates to living data)
   - By operators keyboarding error (breach of integrity within the information chain)
   - Misinformation (communication of false information)
   - Other

3) Accidental leakage of protected data:

   - Inadvertent publication of sensitive information through voice or through social networking sites or by e-mail (misaddress or misdelivery)
   - Information leaked through a P2P exchange service (due to accidental partial or full sharing of workstation resources)
   - Confidential information published on-line following a manipulation error (incident that can be critical when it is about public Web servers)
   - Equipment loss: concerns especially not protected (without password, encryption, etc.) laptop workstations or mobile devices or removable storage devices
   - Document loss
   - Other

4) Programming error (software bugs) leading to system malfunction

   - At infrastructure components level
   - At software products or specific application software level

5) Configuration error leading to system malfunction

   - At infrastructure components level
   - At software products or specific application software level

6) Other

B.1.2.10 Breakdown or malfunction

1) Physical failure: physical or software cause
2) Unavailability due to environmental failure:
   - Internal power supply black-out
   - External power supply black-out
   - Air conditioning failure
   - By electromagnetic waves disturbance
   - Other
3) Abnormal activity:
   - On an application software connections surge
   - Network load unusual increase
   - Unusual server internal load
   - Other

B.1.2.11 Environmental events (unavailability caused by a natural disaster)

1) Water discharge: impact on activity or an IS hardware component with various possible causes (heavy rain, flooding, excessive condensation, etc.)
2) Fire
3) Temperature effects
4) By a spoiling gas infection
5) Other violent disasters: impact on activity or IS hardware architecture with various possible causes (storm, earthquake, tidal wave, lava flow, fluid spill, equipment destruction due to an external event)

B.1.3 How

B.1.3.1 Unauthorized access to a system and/or to information

1) Authentication attacks:
   - Brute force
   - Exploitation of poor credentials (easy to guess)
   - Lack of authentication (i.e. no login)
   - Use of stolen credentials
2) Use of a backdoor that has been installed during the software development stage or in production (after a 1st technical intrusion and installation of malware)
3) Various methods:
   - (OS commanding, LDAP/SQL/XML/e-mail command/etc. injection, buffer overflow, format string, other)
   - Usurpation of functionality (path or directory traversal, cache poisoning, etc.)
   - Encryption attacks (cryptanalysis, encryption brute forcing)

- Protocol manipulation (special unusual commands, HTTP request/response smuggling/splitting)
- Client-side attacks through malware installation (cross-site scripting CSS, man-in-the-browser or man-in-the-middle attacks for theft of cookies)
- Specific methods to access locally to a workstation
- Miscellaneous

4) Nothing to mention

5) Technical methods for the 1st two kinds of events (excluding social engineering techniques to obtain new rights):

- Brute force attack on root (Unix-like systems) and possibly further compromising of other servers
- Exploitation of flaws to trigger buffer overflow and generate privilege escalation
- Access through a compromised workstation to other one with full administrative privileges via a Windows "pass-the-hash" program to finally get shell access on the domain controller
- Miscellaneous

6) Other - Cf. mainly authorization attacks (session replay, cross-site request forgery, exploitation of weak or misconfigured access control, etc.)

B.1.3.2 Unauthorized action on the information system and/or against the organization

1) Illicit partial or full modification of Web homepages content

2) Partial misappropriation of organization's resources (on an internal or security perimeter server) for an external usage by associations providing Warez services on the Internet network

3) Dangerous commands sent to the application or underlying OS

4) Nothing to mention

5) Nothing to mention

6) Nothing to mention

7) Concerns especially passwords or credentials

8) Concerns especially phishing sites

9) Log production and/or retention stopping via specific commands for one of the 2 following reasons: system or application performances improvement at security expense, concealment of an intrusion and/or of unauthorized actions via lack of traces

10) Various methods for various security events:

- Forbidden application transactions carried out by a specialist for the purpose of embezzling funds
- Uncommon application transactions carried out by a specialist for the purpose of embezzling funds
- Interception and rejection of a payment in progress during an EDI type exchange, in order to reproduce the transaction
- Misappropriation of material goods
- User's long and repeated calls, from inside the organization, to a surcharged telephone number in order to run up a fee-based voice server in which s/he has personal interests
- Sale of company's stock options by an employee who holds them, after learning of non-public negative information affecting the company's operations (insider trading)

- Manager's artificial inflating of the figures regarding placed orders in an effort to receive a higher variable compensation (commercial fraud)
- Forgery by an accounting manager in order to conceal operations relating to purchases of useless supplies intended for a company with which s/he is in collusion, in order to indirectly benefit from cash payments by this company
- Corruption of a decision-maker that accesses the requests of a briber in exchange for compensation received on a personal basis (passive bribery)
- Conflict of interest (favoured connection with suppliers, hiring of friends/relatives, etc.)
- Other

11) Various methods for various security events:

- Tax fraud
- Financial misappropriation
- Corruption of a manager by proposing personal benefits to the corrupt person in order to secure a deal (active bribery)
- Fictitious personnel employment
- Interception and rejection of a payment in progress during an EDI type exchange, in order to reproduce the transaction
- Other

12) Means for either events (external attackers) are first intrusions and then specific PABX commands sent to put incoming attacker-generated traffic through to end destinations or to create artificial traffic to fee-based attacker-owned voice servers

13) Repudiation by a customer of a signed or not electronic order (fax, etc.) or modification of a previous not signed electronic order

14) Replay attack possible if no prevention mechanism (one-time message) is used - however infrequent today

15) 2 methods: with a stolen key, without a key through algorithm breaking

16) Nothing to mention

17) 2 situations:

- Employee's usage, with full knowledge of the facts, of the goods, credit, powers, name, brands or voices of his/her company, for direct or indirect personal purposes
- Company employee's misappropriation, at the expense of a third party, of funds, securities or assets provided to him/her and that s/he had accepted, in exchange for an agreement to return them, to represent them or to make a specific usage of them

18) Situation triggered often by fear of telling a undesirable truth

19) Other

B.1.3.3 Installation of unauthorized software programs (malware) on a system (without the owner's consent)

1) Initial installation (on workstations or servers) through various means:

- Opening a malware-loaded attachment (for example Office or pdf document) in an e-mail message or via instant messaging

- Connection to a malware-infected external Web site exploiting a browser software flaw ("drive-by" infection) - may be targeted towards most visited Websites for a given organization ("water-hole"-like attack)
- Downloading of an infected file on an external Web site (via social engineering enticement techniques or not)
- Connection on a workstation of an infected portable storage device via an "auto-exec" feature (USB stick, CD-Rom, …)
- Malware planted on a server after an intrusion or via a remote authorized access (malware programmed into system/software or not)
- Installation by other malware
- Installation via an infected file (via P2P or file sharing)
- Other

  Spreading through various means:

  - Network via a software flaw
  - Sending of e-mail messages using local directories
  - Other

2) Idem above
3) Idem above
4) Similar initially to adware, with downloading of a malware similar to those of category 2 or 3
5) Easier installation (generally without human interaction) than a malware of the 3 first categories
6) Various methods similar to those above

B.1.3.4 Information system remote disturbance

1) DoS methods:
   - Plain smurf-type attack
   - Exploitation of software flaws
   - Benchmark-type procedure injection in a SQL data base (to saturate it)
   - XML attribute blow-up (SOAP architecture)
   - Account lockout attack
   - Other

   DDoS methods:
   - Sending of multiple commands through a network of bots
   - Via public DNS amplification
2) Spam: sending by attacker (often through a network of bots) of a very high rate of messages to hinder regular messaging system operations

   Sending of very oversized messages or attached pieces (nothing to mention)
3) Nothing to mention

B.1.3.5 Social engineering attacks

1) Spear phishing or whaling: reception of customized and spoofed e-mails impersonating authorities or usual relations (such as official State agencies or business partners or fellow users) to entice the recipient to do something harmful to their organization or to him/her

   Organization's call centre operator on the phone deceitfulness: invented and credible scenario to deceive target (pretexting)

   Deceitfulness of mobile phone users: reception of SMS messages to entice the recipient to do something harmful to their organization or to him/her

2) Nothing to mention

3) Ransomware: technical (or not technical) means include:

   - Threat to withhold the encryption key that allowed the attacker, after an intrusion into the server, to encrypt one of the organization's files that can now not be used
   - Threat of a DDoS attack
   - Threat to disclose the previously stolen personal data of its customers
   - Other

     Scareware: see clause B.1.3.3.4)

4) Nothing to mention

5) Hoax: spreading of false (and generally harmless) news on various electronic media

   Scam: similar to clause B.1.3.6.1) with a difference related to the brought about action which is associated to money extortion

6) Nothing to mention

B.1.3.6 Personal attack on organization's personnel or organization disturbance

1) Comments (for last 2 events): abuse of one's situation to get any advantage by easiness or by greed

2) Comments: abuse of one's situation to get any advantage by easiness or by greed

3) Comments (for all events): excessive (impossible to be met) requirements leading to organization disturbance

B.1.3.7 Physical intrusion or illicit action

1) Nothing to mention

2) Documents easy to rob by insiders on messy desks

3) Physical intrusion into organization's premises by unknown persons often achieved through some techniques of visitors welcome hostesses deceitfulness

4) Idem above

5) idem above

6) Concerns notably for information theft Pay at the Pump terminals, Automated Teller Machines (ATM), Point-of-Sale (POS) terminals, etc. via installation of hidden magnetic cards ID number and PIN reader devices

7) Physical proximity and electromagnetic signals pick-up device required

B.1.3.8 Illicit activity carried out on the public Internet network (harming an organization)

1) Registration of a domain name corresponding with a name or brand to which no legitimate rights are held, for the sole purpose of preventing the name from later being assigned to its natural holder

2) Attack on a public DNS (by exploiting a software flaw) intended to insert a different address in the place of a legitimate IP address that corresponds with an existing domain, in order to divert users wishing to access the legitimate website from another site. Other possible objective: create an illegitimate IP address that corresponds with a non-official domain name, in order to avoid payment or any verification

3) Total or partial duplication of a Website through systematic copying of its pages (mirroring)

4) See clause B.1.3.5.1 (same method)

5) Unwitting or malicious and motivated search using keywords targeted towards confidential or personal information) access and leak made possible through an accidental openness and/or sharing of resources on a user workstation P2P client

6) Nothing to mention

B.1.3.9 Various errors (administration, handling, programming, general use)

1) Nothing to mention

2) Nothing to mention

3) Some similar situations of easy to make mistakes with sometimes serious consequences (to be recognized by everybody through user awareness and to be mitigated or avoided by some policies and procedures)

4) Nothing to mention

5) Nothing to mention

6) Nothing to mention

B.1.3.10 Breakdown or malfunction

1) Nothing to mention

2) Nothing to mention

3) Nothing to mention

B.1.3.11 Environmental events (unavailability caused by a natural disaster)

1) Nothing to mention

2) All causes taken into account (accidental only)

3) Causes are mainly: overheated room due to an increase of the outdoor temperature (sun behind the glass, etc.), local overheating due to amplified sun (effect of amplification glass power)

4) Nothing to mention

5) All other natural and natural causes

B.1.4 Status

B.1.4.1 Security event attempt (or occurrence) underway

1) Preparation (applicable only to malice): preliminary actions necessary to launch an attack (such as network reconnaissance or security intelligence collection)

2) Underway: attack launched or event set in

B.1.4.2 Succeeded (or performed) security event

1) Target reached with real CIA consequences

B.1.4.3 Failed security event

1) Event stopped before target hitting

2) Event thwarted by existing measures before target hitting

B.1.5 With what vulnerability(ies) exploited (up to 3 combined kinds of vulnerabilities)

B.1.5.1 Behavioural vulnerability

1) See clause B.2.1.1.

B.1.5.2 Software vulnerability

1) See clause B.2.1.2.

B.1.5.3 Configuration vulnerability

1) See clause B.2.1.3.

B.1.5.4 General security vulnerability

1) See clause B.2.1.4.

B.1.5.5 Conception vulnerability

1) See clause B.2.1.5.

B.1.5.6 Material vulnerability

1) See clause B.2.1.6.

B.1.6 On what kind of asset

B.1.6.1 Data bases and applications

1) Perimeter
   - Enterprise standard application (ERP, supply chain, etc.)
   - Web (bespoke or not) application
2) Internal
   - Data base or data warehouse
   - Enterprise standard application (ERP, supply chain, etc.)
   - Web (bespoke or not) application
3) Public cloud
   - Data base or data warehouse
   - Enterprise standard application (ERP, supply chain, etc.)

- Web (bespoke or not) application

4) Outsourcing (remotely)
   - Data base or data warehouse
   - Enterprise standard application (ERP, supply chain, etc.)
   - Web (bespoke or not) application

B.1.6.2 Systems

1) Perimeter
   - Authentication server
   - Chat/instant messaging server
   - Mail server
   - FTP server
   - File server
   - Fax server
   - Print server
   - DNS server
   - DHCP server
   - Directory server (LDAP, AD, etc.)
   - Log server
   - Server (Windows, Unix-like, other)
   - Web server
   - Terminal services server
   - Remote access server
   - Other
2) Internal
   - Authentication server
   - Chat/instant messaging server
   - Mail server
   - FTP server
   - File server
   - Fax server
   - Print server
   - DNS server
   - DHCP server
   - Directory server (LDAP, AD, etc.)
   - Log server

- Software distribution server
- Server (Windows, Unix-like, other)
- Web server
- Mainframe
- POS control unit
- Terminal services server
- SCADA system (Supervisory Control and Data Acquisition)
- Security secret keys
- Other

3) Public cloud
   - Authentication server
   - Chat/instant messaging server
   - Mail server
   - FTP server
   - File server
   - Fax server
   - DNS server
   - DHCP server
   - Server (Windows, Unix-like, other)
   - Web server
   - Mainframe
   - Security secret keys
   - Other

4) Outsourcing (remotely)
   - Authentication server
   - Chat/instant messaging server
   - Mail server
   - FTP server
   - File server
   - Fax server
   - DNS server
   - DHCP server
   - Directory server (LDAP, AD, etc.)
   - Log server
   - Unix server

- Windows server
- Other server
- Web server
- Mainframe
- Terminal services server
- Security secret keys
- Other

B.1.6.3 Networks and telecommunications

1) Low level devices
   - Router
   - Switch
   - Hub
   - VoIP switch
   - PABX
   - LAN
   - Modem
   - VPN gateway
2) High level communication
   - EDI
   - Proxy
   - Reverse proxy
3) Middleware
   - Storage Area Network (SAN)
   - Gateway to mainframe
   - Machine to Machine protocol
   - Transactional engine
4) Wireless devices
   - Wireless LAN
   - Wireless access point
5) Security
   - Firewall
   - IDS/IPS
   - SSO system

B.1.6.4 Offline storage devices

1) Paper
2) Electronic devices
   - USB sticks
   - Smart cards
3) Magnetic devices
   - External hard disk
   - Backup tapes
   - Media player/recorder
4) Optical devices
   - Disks (CDs, DVDs)
   - Other

B.1.6.5 End-user devices

1) Local application software (user or organization-owned)
   - Office automation standard packages
   - Enterprise bespoke applications
   - Security secret keys
   - Other
2) Multipurpose workstations (user or organization-owned)
   - Desktop (Windows, Mac, Unix-like, other)
   - Laptop (Windows, Mac, Unix-like, other)
3) Dedicated devices (user or organization-owned)
   - Telephone
   - VoIP phone
   - Mobile phone
   - Smart phone
   - PDA
   - Printer/copier/scanner/fax
   - PIN entry device/Card reader
   - User authentication device
   - Automatic Teller Machine (ATM)
   - Pay at the Pump device
   - POS terminal
   - Other

B.1.6.6 People

1) Employee
   - Administrator
   - Maintenance
   - Operator
   - Software developer
   - Manager
   - Executive
   - End-user
   - Other
2) Business partner
   - Supplier
   - Reseller or distributor
   - End-user customer
3) On-premises or off-premises service provider
   - Administrator
   - Maintenance
   - Operator
   - Manager
   - Software developer
   - Other

B.1.6.7 Facilities and environment

1) Real estate
   - Building
   - Physical barrier (windows, doors)
   - Other
2) Physical security devices or systems
   - HVAC system (Heating, Ventilation, Air-Conditioning)
   - Fire suppression system
   - Camera or video device
   - Physical safe
   - Physical access control system
   - Other

3) Various utilities

- Uninterruptible power supply
- Power infrastructure
- Other utilities infrastructure

4) Office furniture

B.1.7 With what CIA consequences

B.1.7.1 Loss of confidentiality (with types of loss and with the amount of data as a possible complement)

1) Personal identifiable information

- Employee
- Customer
- Service provider
- Business partner

For each case, the following choices are the following:

- Full name (if not common)
- First or last name (if common)
- Country, state, or city of residence
- National identification number
- IP address (in some cases)
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card number
- Bank account number
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- Age (especially if non-specific)
- Gender or race
- Name of the school they attend or workplace
- Grades, salary, or job position
- Political opinions
- Criminal record

- Medical information
- Other

2) Professional secrecy
   - Lawyer
   - Bank
   - Insurance
   - Human resources
   - Other
3) Sensitive data (strategic plans, detailed internal financial reports, etc.)
4) Intellectual property
5) Defence classified
6) Network and systems
   - Network topology and addresses
   - Directory
   - Configuration
   - Other
7) Security
   - Authentication credentials
   - Secret keys
   - Other

B.1.7.2 Loss of integrity (with types of loss)

The different possible cases are too diversified to give a complete list. They range from financial fraud to Web defacement to accidental technical modification.

B.1.7.3 Loss of availability (with types of loss and with the duration as a possible complement)

1) Performance decrease
2) Full breakdown or malfunction (interruption without destruction or deletion)
   - Immediate and easy possible recovery
   - No immediate and no easy recovery
3) Deletion
   - Immediate and easy possible recovery
   - No immediate and no easy recovery
4) Physical destruction
   - Recovery possible
   - No recovery possible

5) Physical loss or theft

B.1.8 With what kind of impact

B.1.8.1 Direct impact

1) Disruption to business operations
   - Increased operating costs
   - Turnover cut
   - Other
2) Loss of productivity
3) Fraud
   - Money
   - Other
4) Incident recovery costs
   - Technical individual time
   - Asset replacement
   - Other
5) Life or health consequences

B.1.8.2 Indirect impact

1) Loss of competitive advantage
   - R&D leak
   - Product or market strategy leak
   - Other
2) Reputation damage
3) Loss of market share
   - Brand damage consequences
   - Downgraded competitive advantage
4) Legal and regulatory costs

B.2 Vulnerabilities

B.2.1 What

B.2.1.1 Behavioural vulnerabilities

1) Illicit or dangerous protocols used
   - Unsecured communication (not ciphered and/or no time-out and/or poor authentication means, etc.) set up to get access to an Internet-facing organization-owned and managed server or application making it possible an unauthorized access

- P2P client installed and set up on a professional workstation in order to use the associated service with the risk of partial or full sharing of the workstation content
- VoIP client installed and set up on a professional workstation in order to use the peer-to-peer service
- Outbound user connection set up to get later remote access to the organization's internal network without using an inbound VPN link and a focal access point
- Remote or local connection to the organization's internal network from a roaming laptop or workstation that is organization-owned and is configured with weak parameters
- System or application accessed through automatic login (instead of manual) by an external service provider, as part of a remote management connection (excluding Internet)
- System or application located within a trusted area accessed from a trusted area via an unprotected area without a secure protocol
- Other unwanted or unsecure or dangerous protocols set up with similar behaviours

2) Internet illicitly accessed

- Internet sites accessed from a professional and enterprise network by communication channels that bypass the outbound security devices, to prevent user tracking which makes up generally the main underlying motivation; for example, Internet access from a perimeter area, tunnelling (SSL port 443), straight access (via an ADSL link or a public Wi-Fi access point and the telephone network), access via a Smartphone connected to the workstation
- Anonymization proxy used to access the Internet from a professional workstation, in order to maintain free access and to avoid organization's filtering of access to forbidden websites
- Other

3) Files illicitly transferred between the organization and the outside world

- Untrusted files downloaded to a professional workstation from an external Website unknown (with no reputation within the profession)
- Personal public instant messaging account used to exchange business files with the outside world
- Personal http-based (webmail) public messaging account used to exchange business files with the outside world
- E-mail sent to an address outside of the organization with a confidential and unencrypted attachment
- Other

4) Workstation used without complying the required security tools, configurations and rules

- Workstation used with disabled or out-of-date AV and/or FW
- Secured workstation unsecured (for example, auto run enabled or boot with external device unlocked or lack of timeout)
- Professional workstation configured or accessed in administrator mode without authorization
- Messaging system accessed from a workstation used or configured in administrator mode
- Public Internet accessed from a workstation used or configured in administrator mode
- Personal storage devices (USB stick, CD-ROM, floppy, digital camera, etc.) connected to a professional workstation to exchange information or software
- Use of a BYOD personal device missing basic security measures intended to compartmentalize professional activities from personal ones (or use with such security measures disabled)
- Sensitive files not ciphered loaded from a professional workstation on professional mobile or removable storage devices

- Presence on a professional workstation of personal software that does not comply with corporate security policy
- Presence on a professional or personal workstation of personal software protected by copyright without purchasing a licence (pirated software)
- Files unwittingly shared as regards a P2P client installed in a workstation
- Desktop workstation not turned off when leaving its office
- Laptop workstation used outside the organization without encrypted confidential data
- Not attended by user unprotected equipment (laptop workstation or removable storage device)
- Other

5) Password illicitly handled or managed

- Weak password used
- Password not changed in due time (in case of changes not periodically required)
- Password not changed in due time by an administrator in charge of an account used automatically by systems or applications (in case of changes not periodically required)
- Invalid password used, although already used in the past and/or still used elsewhere
- Password neglected in its protection (for example, password written on a medium and easily accessible)

6) Authentication illicitly handled or managed

- Non-compliant weak authentication permanently used (temporarily authorized instead of the strong authentication required as a result of loss or forgetting of the badge)
- Other

7) Access rights illicitly granted

- User right not compliant granted by an administrator outside any official procedure (with malicious intent or through error or negligence)
- User right not compliant granted by an administrator (through weakness and outside of any official procedure) to managers due to pressure from them

8) Central systems or applications irrelevantly handled

- Logging out of a system or an application overlooked
- Unprotected sensitive data accessed from an unprotected location
- Confidential documents printed on a distant shared printer with documents not being immediately retrieved
- Multiple identifiers used within the organization (in the case of existence of a single directory and of centralized ID and access management)
- Not attended unprotected security management terminal
- Operation involving a firewall or gateway carried out negligently by a network administrator's (dangerous modification of the open ports and of the configuration)
- Other

9) Weakness exploited through social engineering methods

- Human weakness exploited by a spear phishing message meant to entice users to trigger actions that are possibly harmful to the organization (typically clicking on a public Internet link or opening an attached document)

- Human weakness exploited through conversations leading to disclosure of secret information; it typically relates to phone discussions leading to leak of personal identifiable information (PII) or various business details to be used later (notably for identity usurpation)
- Other

10) Miscellaneous

- IT files on a physical medium (DAT, CD-ROM, etc.) sent without encryption to an external service provider by carrier or delivery person
- Within the framework of exchanges with an external service provider, decryption key delivered to a service provider's employee without the latter having signed a confidentiality agreement
- Sensitive assets (laptop workstation or strong authentication device) not or partially returned in case of departure from one's position
- Organization's security policy application rebuffed (while insufficiently justified) by a high-level manager who is abusing his/her authority
- Other

B.2.1.2 Software vulnerabilities

No classification is proposed for this category, since a well-established and world-wide practice exists with the CWE identification scheme (see NIST SP 800-126 Revision 2 [i.1] - Cf. SCAP). Annual surveys (such as the SANS Institute one) generally list top weaknesses categorizing them into high-level categories such as:

- Insecure interaction between components
- Risky resource management
- Porous defences

These weaknesses stem from widespread and critical errors in software development, and their knowledge may act as a tool for education and awareness to help programmers to prevent the kinds of vulnerabilities that plague the software industry.

B.2.1.3 Configuration vulnerabilities

No classification is proposed for this category, since a well-established practice exists with the CCE (Common Configuration Enumeration) List (see MITRE CCE Version 5 [i.2]). Standard secure configurations are available for major OS (Unix-like and Windows), browser (IE), Internet server (WebLogic), application (Office) or cross-platform best practices. Entries in the CCE List contain the following attributes:

- CCE Identifier Number;
- Description;
- Conceptual Parameters;
- Associated Technical Mechanisms;
- References.

Based on these extensive lists, it is obvious to derive configuration vulnerabilities that can be also considered as non-conformities against the best practices. It should be also added to these lists other configuration vulnerabilities regarding (fixed or wireless) network security. A list is given below:

- External router configuration (possible switching to a destination other than the external firewall)
- Transmission at the exit from the external firewall (use of a protocol other than FTPS)
- Absence of the https protocol in the connection between an organization's external router and a reverse proxy

- Absence of filtering of dangerous communication protocols (P2P, inbound FTP, certain r-commands on UNIX, Telnet, shareware programs, etc.) for exchanges with outside the organization
- Remote connection means from an external software development service provider to the organization's network other than by the authorized means (for example, specialized connections or partitioning of the flows on a shared link)
- Not compliant configuration of a firewall's security rules
- Not compliant list of users authorized to access the firewall
- Wi-Fi network with non-existent or insufficient security protocol (WEP activated, for example)
- Lack of secure protocol for transfer of security or sensitive data between 2 servers
- Encryption of internal or external exchanges without strong cryptographic means
- Absence of caller identification in the VoIP protocol of a telephone system
- Other

These lists of configuration vulnerabilities can be used to implement state-of-the-art security policies which can be considered what organizations need to get efficient preventative measures.

B.2.1.4 General security (organizational) vulnerabilities

1) Security organization
   - Sensitive security position held by a person not appointed in an official internal document
   - Unappointed sensitive security position
   - Non-existent position memo
   - Other
2) Governance
   - Decision regarding ISMS improvement (according to the PDCA model) made on the basis of a largely irrelevant operational indicator during a steering committee meeting
   - Lack of sufficiently precise experience feedback and of ISMS improvement proposals
   - Lack of assessment of the cost of a security incident during a meeting about the lessons to be learned from this incident
   - Insufficient user awareness-raising (based on security-related behaviour indicators)
   - Other
3) Development and testing
   - Launch of new projects without information classification
   - Launch of specific bespoke new projects without performing a complete risk assessment
   - Launch of new projects of a standard type without identification of vulnerabilities and threats and of related security measures
   - Secure development rules not applied
   - Absent or insufficient partitioning between development and testing activities
   - Absent or insufficient partitioning between the testing and IT operational activities
   - Use of production PII data to work out testing samples to be used in testing and preproduction environments without Anonymization

- Projects with discrepancies identified at security level between the release of the development teams and the commissioning
- Absence of periodic IT backups (stored in a waterproof and fireproof safe for magnetic media) by an external software development service provider, or of regular backups on a secure backup site
- Other

4) Security operations

- System and software secure configuration application process not enforced appropriately
- Right management process not enforced appropriately
- Cryptography and key management process not enforced appropriately
- Product and software versions management process not enforced appropriately
- Absence of wiping of personal data or of organization's files from media (used by an external service provider), at the end of the media use or at the end of the service
- Duplication or transmission of organization's files to an external service provider without organization's formal approval
- Other

5) Incident detection and management process

- SIEM tool with partial coverage and poor configuration
- Absence of monitoring of the presence of certain sensitive outgoing flows (http, SSL, instant messaging, P2P, chat, etc.)
- Lack of checking of third party services
- Insufficiently formalized incident handling process for some types of incidents
- Critical incident detected and not declared
- Abnormally high rate of anomalies (incidents that cannot be qualified enough and categorized)
- Critical incident without launched reaction plan
- Standard pre-established reaction plans launched without experience feedback
- Standard pre-established reaction plans unsuccessfully launched
- Abnormally very low rate of successfully launched reaction plans
- Other

6) Vulnerability or weakness detection and management process

- Absence of evaluation of potential vulnerabilities for a sensitive application
- Lack of checking of passwords strength (can be easily guessed by a third party, etc.)
- Poor detection process for vulnerabilities (for example, insufficient frequency of scans)
- Serious weaknesses detected but not declared in a timely manner
- Serious weaknesses detected but not quickly taken into account
- In a MMI, display of non-truncated or non-masked personal data (while display not being necessary for completion of user tasks)

- Situation in which the duration of the window of risks exposure exceeds the time limit expressed in security policy (period of time between the public disclosure of a critical software vulnerability and the actual and checked application of a patch that corresponds with the vulnerability's correction)
- Abnormally high rate of not patched systems for detected critical software vulnerabilities
- Abnormally high rate of not reconfigured systems for detected critical configuration vulnerabilities
- Other

7) Auditing process

- Abnormal respective success rates for periodic auditing / continuous auditing
- Incomplete or excessively superficial review of user accounts
- Difficult to use operational indicator for measuring security policy effectiveness or application level
- Other

8) Miscellaneous

- Absence of an owner for an application or system
- Other

NOTE: **General security technical vulnerabilities** are not addressed in this taxonomy since they do not bring enough added value against the ISO 27002 [i.7] relevant points of control.

B.2.1.5 Conception vulnerability

1) Software

- Immature or new software
- Lack of audit trail
- No or insufficient software testing
- Unprotected password tables
- Other

2) General design

- Too weak authentication (password-only)
- Poor credentials management
- Reuse of storage media without proper erasure
- Complicated user interface
- Lack of security review upstream
- Other

3) Environment

- Lack of environmental favourable conditions
- Other

B.2.1.6 Material vulnerability

1) Hardware

- Insufficient maintenance of storage media

- Lack of periodic replacement schemes
- Susceptibility to humidity or dust or soiling
- Sensitivity to electromagnetic radiation
- Lack of efficient configuration change control
- Susceptibility to temperature variations
- Unprotected storage
- Lack of care at disposal
- Uncontrolled copying
- Other

2) Network and systems
   - Lack of back-up
   - Inadequate network management (resilience of routing)
   - Unprotected electronics or power
   - Other
3) Personnel and site
   - Lack of or insufficient security training
   - Lack of security awareness
   - Unsupervised work by cleaning staff
   - Inadequate recruitment procedures
   - Lack of or failure of physical access control to buildings and rooms
   - Lack of physical protection of the building, doors and windows
   - Other
4) Environment
   - Unstable power grid
   - Location in an area susceptible to flood
   - Other

B.2.2 On what kind of assets

See clause B.1.6.

B.2.3 Who (only for behavioural vulnerabilities)

See clause B.1.1.

B.2.4 For what purpose (only for behavioural vulnerabilities)

See clause B.1.2.

B.2.5 To what kind of possible exploitation

See clause B.1.3.

Annex C (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Gerard Gaudin, G²C, Chairman of ISG ISI

Other contributors:
Herve Debar, Institut Telecom, newly appointed Vice-Chairman of ISG ISI

Frederic Martinez, Alcatel-Lucent, newly appointed Secretary of ISG ISI

And in alphabetical order:

Christophe Blad, Oppida

Philippe Bramaud, CEIS

Eric Caprioli, Caprioli & Associés

Erwan Chevalier, BNP Paribas

Paolo De Lutiis, Telecom Italia

Jean-François Duchas, Bouygues Telecom

Gene Golovinski, Qualys Inc.

François Gratiolet, Qualys Inc.

Philippe Jouvellier, Airbus

Stéphane Lemée, Airbus

Stéphane Lu, BNP Paribas

Jean-Michel Perrin, Groupe La Poste

Axel Rennoch, Fraunhofer Fokus

Laurent Treillard, CEIS

Annex D (informative): Bibliography

- MITRE CEET V1.0a: "A Standardized Common Event Expression for Event Interoperability (Common Event Expression Taxonomy)".
- MITRE CAPEC List V1.7.1 (April 2012): "Common Attack Pattern Enumeration and Classification".

List of figures

History

Document history		
V1.1.1	April 2013	Publication
V1.2.1	November 2015	Publication